

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-111545

(43)Date of publication of application : 20.04.2001

(51)Int.Cl.

H04L 9/32

G06F 15/00

G06F 17/60

H04Q 7/38

(21)Application number : 2000-185867

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 21.06.2000

(72)Inventor : KIMURA KYOYA  
IKEDA TAKESHI

(30)Priority

Priority number : 11219739

Priority date : 03.08.1999

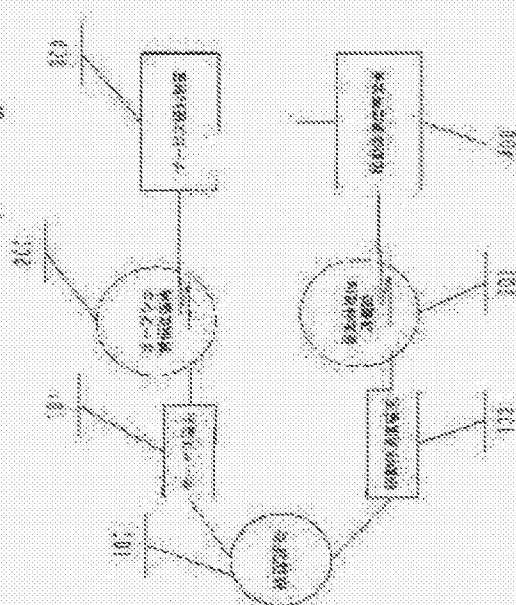
Priority country : JP

## (54) AUTHENTICATING METHOD AND DEVICE THEREOF

(57)Abstract:

PROBLEM TO BE SOLVED: To provide individual authentication system to intensify security without excessively complicating the service, when the service is provided using the Internet, etc.

SOLUTION: A service providing device 300 is provided with a member data base 310, to store information about members registered in advance as object persons of service, a fundamental authenticating means 321 to authenticate the members by using an open information communication path 202 and a mobile object communication way authenticating means 322 to execute authentication via a mobile object communication terminal 102 registered in advance in the member data base 310, a service terminal 101 connected with the service providing device 300 by the open information communication path 202 and the mobile object communication terminal 102 registered in the member data base 310 on the side of a person 10 to be authenticated, and authentication is performed with two communication paths as the open information communication path 202 and a mobile object communication path 201 by this structure.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

(10) 日本特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2001-111545  
(P2001-111545A)

(43) 公開日 平成13年4月20日 (2001.4.20)

(51) Int.Cl. <sup>7</sup>	識別記号	FI	ナニダ(参考)
H04L 9/32		C06F 15/00	330B
G06F 15/00	330		330C
		17/00	332
17/00	332		506
	506	H04L 9/00	573A

審査請求 未請求 請求項の数 6 O/L (全 40 頁) 最終頁に続く

(21) 出願番号 特願2000-185967(P2000-185967)

(22) 出願日 平成12年6月21日 (2000.6.21)

(31) 優先権主張番号 特願平11-219739

(32) 優先日 平成11年8月3日 (1999.8.3)

(33) 優先権主張国 日本 (JP)

(71) 出願人 00093221

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 本村 泰也

神奈川県川崎市多摩区東三田3丁目10番1号 松下技研株式会社内

(73) 発明者 池田 健

大阪府門真市大字門真1006番地 松下電器産業株式会社内

(74) 代理人 10009/445

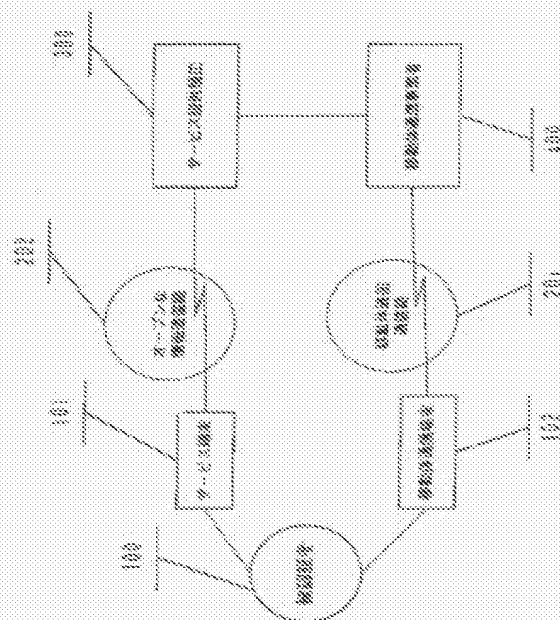
弁護士 岩崎 文雄 (外2名)

## (54) 【発明の名称】 認証方法及びその装置

## (57) 【要約】

【課題】 インターネット等を用いてサービスを提供する場合に、過度に複雑化することなくセキュリティを強化する個人認証システムの提供を目的とする。

【解決手段】 サービス提供装置300は、サービス対象者として事前登録されている会員の情報を記憶する会員データベース310と、オープンな情報通信路202を用いて会員であることを認証する基本認証手段321と、会員データベース310に事前に登録した移動体通信端末102を経由した認証を実行する移動体通信経路認証手段322とを備え、被認証者100は、サービス提供装置300とオープンな情報通信路202で接続されたサービス端末101と、会員データベース310に登録されている移動体通信端末102を備えており、この構成により、オープンな情報通信路202と移動体通信経路201の2つの通信経路で認証を行うことが可能となる。



## 【特許請求の範囲】

【請求項1】 被認証者から、サービス受給者を識別する会員ID信号の情報をオープンな情報通信路から受け取るステップと、

サービスの提供を受けられる会員の情報を登録した会員データベースの情報と前記課金認証管理手段から受け取った前記会員IDとを照合して、会員を識別するステップと、

前記会員が識別された場合、前記会員データベースに登録されている前記会員IDに対応して登録されている被認証者用の移動体通信端末の番号に対して接続要求をおこなうステップと、

前記移動体通信端末より認証の了承の信号を受け取った場合、認証がされたと判定するステップとを有する認証方法。

【請求項2】 サービスの提供を受けられる会員の情報を登録した会員データベースと、

被認証者から、サービス受給者を識別する会員ID信号の情報をオープンな情報通信路から受け取る個人認証管理手段と

前記会員データベースに登録されている情報と前記個人認証管理手段から受け取った前記会員IDとを照合して、会員を識別する基本認証手段と、

前記基本認証手段で、前記会員IDが認証された場合、前記会員データベースに登録されている前記会員IDに

対応して登録されている被認証者用の移動体通信端末の番号に対して接続要求をおこなう移動体通信経由認証手段とを有し、

前記移動体通信端末より認証の了承の信号を受け取った場合、認証がされたと判定する認証装置。

【請求項3】 サービスを提供する施設から、前記設備を認識する識別信号をオープンな情報通信路をから受け取り、その設備を識別するステップと、

前記設備が識別された場合、前記サービスを利用したサービス受給者から前記サービス受給者を識別する識別信号及び前記サービスの料金をオープンな情報通信路から受け取るサービス受給者を識別するステップと、

サービス受給者が識別された場合、あらかじめデータベースに登録されている課金対象者の移動体通信端末の番号に照線接続を行い、前記課金対象者に、前記料金の支払いの可否を問い合わせるステップと、

前記移動体通信端末より、前記課金対象者が前記料金の支払いを了承した信号を受け取った場合、前記データベースに課金額を登録し、あらかじめ登録されている決済口座よりその課金額を引き落とすステップとを有する課金方法。

【請求項4】 サービスを提供する施設の情報を登録したデータベースと、

サービスの提供を受けられる会員の情報を登録した会員データベースと、サービスを提供する施設から、前記施設

を識別する施設ID信号、サービス受給者を識別する会員ID信号及び前記サービスに関する課金額の情報をオープンな情報通信路から受け取る課金認証管理手段と、

あらかじめ施設データベースに登録されている情報と前記課金認証管理手段から受け取った前記施設ID信号を照合して前記施設を識別する施設認証手段と、

前記会員データベースに登録されている情報と前記課金認証管理手段から受け取った前記会員IDとを照合して、会員を識別する基本認証手段と、

前記基本認証手段で、前記会員IDが認証された場合、前記会員データベースに登録されている課金対象者の移動体通信端末に対して接続要求をおこなう移動体通信経由認証手段と、

前記課金対象者の移動体通信端末から前記課金額に対して了承の信号を受け取った場合、

あらかじめ登録されている決済口座より前記課金額を引き落とす課金手段とを有する課金装置。

【請求項5】 サービス受給者を識別する会員ID及び前記サービスに関する課金額の情報をオープンな情報通信路から受け取るステップと、

サービスの提供を受けられる会員の情報を登録した会員データベースと前記会員IDとを照合し、サービス受給者が識別された場合、あらかじめデータベースに登録されている課金対象者の移動体通信端末の番号に照線接続を行い、前記課金対象者に、前記料金の支払いの可否を問い合わせるステップと、

前記移動体通信端末より、前記課金対象者が前記料金の支払いを了承した信号を受け取った場合、前記データベースに課金額を登録し、あらかじめ登録されている決済口座よりその課金額を引き落とすステップとを有する課金方法。

【請求項6】 サービスの提供を受けられる会員の情報を登録した会員データベースと、

サービス受給者を識別する会員ID信号及び前記サービスに関する課金額の情報を前記会員からオープンな情報通信路から受け取る課金認証管理手段と、

前記会員データベースに登録されている情報と前記課金認証管理手段から受け取った前記会員IDとを照合して、会員を識別する基本認証手段と、

前記基本認証手段で、前記会員IDが認証された場合、前記会員データベースに登録されている課金対象者の移動体通信端末に対して接続要求をおこなう移動体通信経由認証手段と、

前記課金対象者の移動体通信端末から前記課金額に対して了承の信号を受け取った場合、あらかじめ登録されている決済口座より前記課金額を引き落とす課金手段とを有する課金装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子商取引やパソコン通信等、情報通信を用いてサービスを実現するシステムの個人認証をより確実にする個人認証システムに関するものである。

【0002】

【従来の技術】従来より、電子的手段を用いての契約、取り引き等が行われる場合に、その電子的手段を用いている者が正規の契約者であるか否かの認証は、暗証番号、パスワード等によって行われてきた。例えば、パソコン通信の場合であれば、パソコンおよび電話回線を用いてパソコン通信の会員が契約申し込み情報を送信し、パソコン通信事業者側に設置されたサービス提供装置（サービス提供者が保有するサーバをいう）ではこれを受信することで、その両者間の契約を行ってきた。この際、そのパソコン通信会員に成り済まし、不正な利用者が契約を実行することを排除するための認証手順は次のようなものである。

【0003】まず、予めパソコンユーザとパソコン通信事業者との間で利用契約を締結する。その際、パソコン通信事業者は正規会員ユーザへ会員ID番号、パスワードを通知する。パソコン通信事業者はパソコン通信を介してユーザからアクセス要求があった時には、アクセス要求しているユーザに対して予め登録させた会員IDおよびパスワードを要求し、ユーザがこれを入力した時にパソコン通信事業者側に記録されている正規会員情報と照合して、これに適合したときには、アクセス要求しているユーザを正規の会員ユーザと認証する。そして、この認証により確立された通信路を用いてアクセス者から送信されてくる、注文情報等は、正規の会員ユーザが送信したものと受け付けると言うものである。

【0004】

【発明が解決しようとする課題】しかし、これら従来の技術では、以下のような欠点を有していた。

【0005】従来の個人認証技術では、ハッカーが正規会員ユーザのパソコンの送信ゲート、あるいは、モデム等に侵入し、ここで正規会員ユーザが送信する会員ID番号やパスワードを取得してしまえば、不正利用者による「成り済まし」を排除することは困難である。

【0006】現在、ハッカーによる会員ID番号およびパスワードの不正取得を防止することを目的に、正規会員ユーザとサービス提供者間では、情報の伝達を暗号処理し、通信セキュリティを確保して行われることがある。しかし、パスワード等の不正取得を防止する手段を如何に高度化、複雑化させたところで、より高度な不正取得手段を開発するハッカーに対して従来の個人認証技術は十分安全なものとは言えない。

【0007】また、予め設定された会員IDおよびパスワードも何らかの手段で他者が知った場合は、本人認証としての役割を果たすことはできない。

【0008】本発明は、上記従来技術の課題を解決する

もので、不正利用者により正規会員ユーザの会員ID番号およびパスワードの不正取得が行われたとしても不正利用者による「成り済まし」を排除することが可能な確度の高い個人認証システムの提供を目的とする。

【0009】

【課題を解決するための手段】この課題を解決するために、本発明は、オープンな情報通信路だけでなく、移動体通信事業者の持つ通信路も用いて個人認証を実行するよう構成したものである。これにより、オープンな情報通信路で不正利用者により正規会員ユーザの会員ID番号およびパスワードの不正取得が行われたとしても不正利用者による「成り済まし」を排除することが可能な確度の高い個人認証システムを実現することができる。

【0010】以下、本発明について、図面を参照しながら説明する。

【0011】

【発明の実施の形態】（実施の形態1）図1は本実施の形態における個人認証システムを示す概念図である。図1において、300は、オープンな情報通信路を用いてサービスを提供するサービス提供者が保有するサービス提供装置、100は、認証対象である被認証者、101は、サービス提供装置300から被認証者100へのサービス提供を実現するサービス端末、102は、被認証者100が所持するサービス提供装置300に事前登録されている移動体通信端末、400は、移動体通信端末102を接続するPHS、携帯電話等の移動体通信事業者、202は、サービス端末101とサービス提供装置300を接続し、サービス提供装置300からサービス端末101へサービスを提供するオープンな情報通信路、201は、移動体通信事業者400と移動体通信端末102を接続する移動体通信通信路である。

【0012】ここで、オープンな情報通信路202とはインターネットなど不特定多数のユーザが任意のサービス提供者へアクセス可能な情報通信路を示しており、このオープンな情報通信路202を用いてサービス提供装置300は、例えば、パソコン通信プロバイダサービス、電子商取引サービス等を提供する。

【0013】なお、図1においては、サービス利用者である被認証者100が一人のみ示されているが、一般的応用においては複数の被認証者および複数のサービス端末が存在しており、被認証者100はその内の一人を示すことになる。

【0014】図2は、本実施の形態におけるサービス提供装置300の構成を示す概念図である。図2において、310は、サービス対象者として事前登録されている会員の会員ユーザ情報を記憶する会員データベース、320は、サービス要求を行っているユーザが正規の会員ユーザか否かを認証、判断する個人認証部である。また、個人認証部は、オープンな情報通信路202を用いて会員であることを認証する基本認証手段321と、正



組合員の所持している移動体通信端末を用いて会員であることを認証する移動体通信経由認証手段322と、基本認証手段321および移動体通信経由認証手段322を統括管理し、個人認証の判断を行う個人認証管理手段から構成されている。

【0015】図3は、本実施の形態で示す個人認証システムを実現するために必要な会員ユーザ情報の例を示しており、この会員ユーザ情報は、会員データベース310に事前に登録されている。

【0016】図3には、3名の会員ユーザ情報が記憶されている例を示しており、会員情報の内訳は、「会員氏名」、及び、オープンな情報通信路202経由で認証を行う時に用いる「会員ID番号」、「基本認証パスワード情報」と移動体通信通信路201経由で認証を行う時に用いる「移動体通信端末呼び出し番号」、「移動体通信経由認証パスワード情報」である。

【0017】図4は、本実施の形態で示す個人認証システムの認証手順を示したフローレーション図であり、手順1～手順25の数字は、認証手順の順番を示している。以下、本実施の形態で示す個人認証システムの動作を図4の認証順番毎に説明する。

【0018】<手順1>被認証者100は、図1に示すサービス提供者の保有するサービス提供装置300のサービス提供を受けるために、サービス端末101に、「会員ID番号」及び「基本認証パスワード情報」を入力する。ここで、「会員ID番号」及び「基本認証パスワード情報」とは、被認証者100がサービス提供者とサービス提供契約を交わした際に、サービス提供者から通知されるものであり、通知された前記「会員ID番号」及び「基本認証パスワード情報」は、サービス提供者が保有するサービス提供装置300内の会員データベース310に被認証者100の氏名および被認証者100の所持する移動体通信端末102の移動体通信端末呼び出し番号と対応付けられ記憶されているものとする。

【0019】<手順2>「会員ID番号」及び「基本認証パスワード情報」を入力されたサービス端末101はオープンな情報通信路202を経由して前記「会員ID番号」及び「ユーザ入力基本認証パスワード情報」をサービス提供装置300内の個人認証管理手段へ送信し、サービス提供装置300としての個人認証を要求する。

【0020】ここで、オープンな情報通信路202を使用して前記「会員ID番号」及び「ユーザ入力基本認証パスワード情報」を通信する場合、これらの情報の不正取得を防止することを目的にサービス端末101とサービス提供装置300間では情報の伝達を暗号処理し、通信セキュリティを確保してもよい。また、「ユーザ入力基本認証パスワード情報」とは、ユーザがユーザ端末101から入力した「基本認証パスワード情報」を示す。

【0021】<手順3>個人認証要求および「会員ID番号」「ユーザ入力基本認証パスワード情報」を受信した

個人認証管理手段323は、「会員ID番号」「ユーザ入力基本認証パスワード情報」を基本認証手段321に送付し、「会員ID番号」に対応するサービス対象者の個人認証を要求する。

【0022】<手順4>「会員ID番号」「ユーザ入力基本認証パスワード情報」を個人認証管理手段323から受け取った基本認証手段321は、会員データベース310に対して、個人認証管理手段323より受け取った「会員ID番号」に対応する「照合用基本認証パスワード情報」を要求する。

【0023】ここで、「照合用基本認証パスワード情報」とは、会員データベース310が、記憶している「会員ID番号」に対応した「基本認証パスワード情報」を示している。

【0024】<手順5>会員データベース310は、要求のあった「会員ID番号」をキーワードに、データベース内の会員ユーザ情報の検索を実行し、同一の「会員ID番号」を発見した場合には、この「会員ID番号」に対応する「照合用基本認証パスワード情報」を基本認証手段321へ送付する。

【0025】ここで、検索の結果、要求のあった「会員ID番号」が発見できなかった場合は、会員データベース310は、基本認証手段321へ会員ID番号がないことを通知する。

【0026】<手順6>基本認証手段321は、会員データベース310から「照合用基本認証パスワード情報」が返送されてくると、前記「照合用基本認証パスワード情報」と「ユーザ入力基本認証パスワード情報」を比較照合し、同一であれば、基本認証が成立したと判定し、同一でない場合は、基本認証が不成立であったと判定する。

【0027】ここで、会員データベース310から検索すべき「会員ID番号」が存在しない旨の通知を受けた場合、基本認証手段321は、基本認証が不成立であったと判定する。

【0028】<手順7>基本認証手段321は、「会員ID番号」と共に、基本認証の判定結果を個人認証管理手段323へ通知する。

【0029】<手順8>個人認証管理手段323は、基本認証手段321から送られてきた認証結果が、基本認証成立である場合には、「会員ID番号」を移動体通信経由認証手段322へ送付し、移動体通信経由認証を要求する。

【0030】ここで、基本認証手段321から送られてきた基本認証の結果が、基本認証不成立であった場合、個人認証管理手段323はサービス端末101へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【0031】<手順9>「会員ID番号」を個人認証管理手段323から受け取った移動体通信経由認証手段322

は、会員データベース310に対して、個人認証管理手段323より受け取った「会員ID番号」に対応する「照合用移動体通信経由認証パスワード情報」および「移動体通信端末呼び出し番号」を要求する。

【0032】ここで、「照合用移動体通信経由認証パスワード情報」とは、会員データベース310が、記憶している「会員ID番号」に対応した「移動体通信経由認証パスワード情報」を示している。

【0033】<手順10>会員データベース310は、要求のあった「会員ID番号」をキーワードに、データベース内の会員ユーザ情報の検索を実行し、同一の「会員ID番号」を発見した場合には、この「会員ID番号」に対応する「照合用移動体通信経由認証パスワード情報」および「移動体通信端末呼び出し番号」を移動体通信経由認証手段322へ送付する。

【0034】なお、検索の結果、要求のあった「会員ID番号」が発見できなかった場合は、会員データベース310は、移動体通信認証手段322へ会員ID番号が存在しないことを通知する。

【0035】<手順11>移動体通信経由認証手段322は、会員データベース310から「照合用移動体通信経由認証パスワード情報」および「移動体通信端末呼び出し番号」が送達されてくると、移動体通信事業者400に対して「移動体通信端末呼び出し番号」を使用して移動体通信端末102への回線接続要求を行う。なお、移動体通信経由認証手段322が、会員データベース310から検索すべき「会員ID番号」が存在しない旨の通知を受けた場合、移動体通信手段322は、基本認証が不成立であったと判定し、手順24へ手続きを進める。

【0036】また、移動体通信経由認証手段322から移動体通信事業者400へ回線接続要求を送信する際使用する通信路は、専用回線あるいは、電話通信網等の公共回線のどちらを使用しても良い。

【0037】<手順12>～<手順15>手順12、手順13、手順14、手順15の操作は、移動体通信事業者400の回線接続方法により異なるが、以下、携帯電話等の一般的な回線接続方法を示す。

【0038】<手順12>移動体通信事業者400は、移動体通信通信路201を用いて移動体通信端末102に対して回線接続要求を行う。ここで、移動体通信端末102が他の通信に使用されている等で回線接続が不可能である場合は、移動体通信事業者400は、回線接続失敗と判定し、手順16へ進む。

【0039】<手順13>移動体通信事業者400から回線接続要求を受けた移動体通信端末102は、回線接続要求を受けていることを被認証者100に呼び出しベル、バイブレータ等を用いて通知する。

【0040】<手順14>被認証者100は、移動体通信端末102に設置されている応答ボタン等を押すことにより回線接続要求に応答する。

【0041】<手順15>移動体通信端末102は、被認証者100から応答があったことを移動体通信通信路201を用いて移動体通信事業者400へ通知し、移動体通信通信路201に回線を設定する。

【0042】<手順16>移動体通信事業者400は、回線接続結果を移動体通信経由認証手段322へ通知する。ここで、移動体通信経由認証手段322は、移動体通信事業者400から送付された回線接続結果が、回線接続失敗であった場合、移動体通信経由認証が不成立であったと判定し、手順24へ進む。

【0043】<手順17>～<手順19>移動体通信事業者400からの回線接続結果が回線接続成功であった場合、移動体通信経由認証手段322は、移動体通信通信路201に設定された回線を用いて「移動体通信経由認証パスワード情報」の入力を被認証者100へ要求する。

【0044】ここで、「移動体通信経由認証パスワード情報」とは、被認証者100がサービス提供者とサービス提供契約を交わした際に、サービス提供者から通知されるものであり、通知された前記「移動体通信経由認証パスワード情報」は、サービス提供者が保有するサービス提供装置300内の会員データベース310に被認証者100の氏名および被認証者100の所持する移動体通信端末103の移動体通信端末呼び出し番号と対応付けられ記憶されているものとする。

【0045】なお、サービス提供契約を交わした正規の会員ユーザ以外の不正利用者が、何らかの方法で正規会員ユーザの「基本認証パスワード情報」および「会員ID番号」を手出し、正規会員ユーザに成り済まし、サービス提供要求をした場合、正規会員ユーザは、前記「移動体通信経由認証パスワード情報」の入力要求を移動体通信端末102から受けることにより、不正利用の要求が行われていることを知る ことができる。

【0046】<手順20>～<手順23>被認証者100が、「移動体通信経由認証パスワード情報」を移動体通信端末102へ入力すると、移動体通信端末102は、移動体通信通信路201に設定された回線を用いて「ユーザ入力移動体通信経由認証パスワード情報」を移動体通信経由認証手段322へ送付する。ここで、「ユーザ入力移動体通信経由認証パスワード情報」とは、ユーザが移動体通信端末102から入力した「移動体通信経由認証パスワード情報」を示す。

【0047】<手順23>移動体通信経由認証手段322は、「ユーザ入力移動体通信経由認証パスワード情報」が送達されてくると、前記「照合用移動体通信経由認証パスワード情報」と「ユーザ入力移動体通信経由認証パスワード情報」を比較照合し、同一であれば、移動体通信経由認証が成立したと判定し、同一でない場合は、移動体通信経由認証が不成立であったと判定する。

【0048】<手順24>移動体通信経由認証手段322

は、「会員ID番号」と共に、移動体通信経由認証の認証結果を個人認証管理手段323へ通知する。

【0049】<手順25>個人認証管理手段323は、移動体通信経由認証手段322から送られてきた認証結果が、移動体通信経由認証の成立である場合には、個人認証が成功したと判定し、サービス提供装置300からサービス端末101へのサービス提供を開始する。

【0050】また、認証結果が、移動体通信経由認証が不成立であった場合、個人認証管理手段323はサービス端末101へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【0051】(実施の形態2)図5は本実施の形態における個人認証システムを示す概念図である。図5において、被認証者100、移動体通信通信路201、オープンな情報通信路202、サービス提供装置300、移動体通信事業者400は、図1に示す実施形態1の個人認証システムと同様の機能を有しており、本実施の形態と実施形態1の個人認証システムとの差異は、本実施の形態で示す個人認証システムでは、個人認証を実施する際、情報通信端末101と移動体通信端末102間を「サービス端末、移動体通信端末間通信路」203を用いて接続する点であり、サービス端末101は、実施の形態1の機能に加え「サービス端末、移動体通信端末間通信路」203とのインターフェース機能、および移動体通信端末102の呼び出しに対して応答する機能が付加されている。

【0052】また、移動体通信端末102も実施の形態1の機能に加え「サービス端末、移動体通信端末間通信路」203とのインターフェース機能を付加されている。ここで、「サービス端末、移動体通信端末間通信路」203とは、有線を用いた接続、無線を用いた接続、あるいは、音響カプラ等を用いた接続路を示す。

【0053】図6は、本実施の形態で示す個人認証システムを実現するために必要な会員ユーザ情報の例を示しており、この会員ユーザ情報は、図2に示す会員データベース310に事前に登録されている。

【0054】図6には、3名の会員ユーザ情報が記憶されている例を示しており、会員情報の内訳は、「会員氏名」、及び、オープンな情報通信路202経由で認証を行う時に用いる「会員ID番号」、「基本認証パスワード情報」と移動体通信通信路経由で認証を行う時に用いる「移動体通信端末呼び出し番号」である。

【0055】図7は、本実施の形態で示す個人認証システムの認証手順を示したコラボレーション図であり、手順1～手順24の数字は、認証手順の順番を示している。以下、本実施の形態で示す個人認証システムの動作を図7の認証手順毎に説明する。

【0056】<手順1>被認証者100は、所持する移動体通信端末102をサービス端末101へ「サービス端末、移動体通信端末間通信路」を用いて接続する。

【0057】<手順2>～<手順9>被認証者100のサービス提供要求から基本認証の成立までは、図4の実施の形態1の個人認証手順<手順1>～<手順8>と同様である。

【0058】<手順10>「会員ID番号」を個人認証管理手段323から受け取った移動体通信経由認証手段322は、会員データベース310に対して、個人認証管理手段323より受け取った「会員ID番号」に対応する「移動体通信端末呼び出し番号」を要求する。

【0059】<手順11>会員データベース310は、要求のあった「会員ID番号」をキーワードに、データベース内の会員ユーザ情報の検索を実行し、同一の「会員ID番号」を発見した場合には、この「会員ID番号」に対応する「移動体通信端末呼び出し番号」を移動体通信経由認証手段322へ送付する。

【0060】なお、検索の結果、要求のあった「会員ID番号」が発見できなかった場合は、会員データベース310は、移動体通信認証手段322へ会員ID番号が存在しないことを通知する。

【0061】<手順12>移動体通信経由認証手段322は、会員データベース310から「移動体通信端末呼び出し番号」が返送されてくると、移動体通信事業者400に対して「移動体通信端末呼び出し番号」を使用して移動体通信端末102への回線接続要求を行う。なお、移動体通信経由認証手段322が、会員データベース310から検索すべき「会員ID番号」が存在しない旨の通知を受けた場合、移動体通信手段322は、基本認証が不成立であったと判定し、手順23へ手続きを進める。

【0062】また、移動体通信経由認証手段322から移動体通信事業者400へ回線接続要求を送信する際使用する通信路は、専用回線あるいは、電話通信網等の公共回線のどちらかを使用しても良い。

【0063】<手順13>移動体通信事業者400は、移動体通信通信路201を用いて移動体通信端末102に対して回線接続要求を行う。ここで、移動体端末102が他の通信に使用されている等で回線接続が不可能である場合は、移動体通信事業者400は、回線接続失敗と判定し、手順17へ進む。

【0064】<手順14>移動体通信事業者400から回線接続要求を受けた移動体通信端末102は、回線接続要求を受けていることをサービス端末101へ「サービス端末、移動体通信端末間通信路」203を用いて通知する。

【0065】<手順15>サービス端末101は、「サービス端末、移動体通信端末間通信路」203を用いて移動体通信端末102に回線接続要求に対する応答を通知する。

【0066】<手順16>移動体通信端末102は、サービス端末101から応答があったことを移動体通信通信路201を用いて移動体通信事業者400へ通知し、移

動体通信通信路201に回線を設定する。

【0067】<手順17>移動体通信事業者400は、回線接続結果を移動体通信経由認証手段322へ通知する。ここで、移動体通信経由認証手段322は、移動体通信事業者400から送付された回線接続結果が、回線接続失敗であった場合、移動体通信経由認証が不成立であったと判定し、手順23へ進む。

【0068】<手順18>移動体通信事業者400からの回線接続結果が回線接続成功であった場合、移動体通信経由認証手段322は、テスト信号を移動体通信事業者400へ送信し、送信したテスト信号を送信テスト信号として記憶する。

【0069】ここで、テスト信号は、乱数等を用いて発生させた任意の信号を用いてもよいし、事前に移動体通信経由認証手段322が記憶している任意の信号を用いてもよい。

【0070】<手順19>移動体通信事業者400は、移動体通信通信路201に設定された回線を用いて前記テスト信号を移動体通信端末102へ送信する。

【0071】<手順20>移動体通信端末102は、「サービス端末、移動体通信端末間通信路」203を用いて前記テスト信号をサービス端末101へ送信する。

【0072】<手順21>サービス端末101は、オープンな情報通信路203を用いて前記テスト信号を移動体通信経由認証手段323へ送信する。

【0073】<手順22>移動体通信経由認証手段323は、前記テスト信号を受信すると、記憶している「送信テスト信号」と受信したテスト信号を比較照合し、同一であれば、移動体通信経由認証が成立したと判定し、同一でない場合は、移動体通信経由認証が不成立であったと判定する。

【0074】<手順23>移動体通信経由認証手段322は、「会員ID番号」と共に、移動体通信経由認証の認証結果を個人認証管理手段323へ通知する。

【0075】<手順24>個人認証管理手段323は、移動体通信経由認証手段322から送られてきた認証結果が、移動体通信経由認証の成立である場合には、個人認証が成功したと判定し、サービス提供装置300からサービス端末101へのサービス提供を開始する。

【0076】また、認証結果が、移動体通信経由認証が不成立であった場合、個人認証管理手段323はサービス端末101へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【0077】(実施の形態3)本実施の形態の構成は、図5に示す実施の形態2の個人認証システムと同様である。また、本実施の形態で示す個人認証システムを実現するために必要な会員ユーザ情報も図6に示す実施の形態2の会員情報と同様である。

【0078】本実施の形態と実施の形態2では、認証手順が異なっており、図8は、本実施の形態で示す個人認

証システムの認証手順を示したコラボレーション図である。ここで、図9の手順1～手順24の数字は、認証手順の順番を示している。以下、本実施の形態で示す個人認証システムの動作を図8の認証順番毎に説明する。

【0079】<手順1>～<手順17>サービス端末101と移動体通信端末102の接続、該認証者100の基本認証成立、および、移動体通信通信路201上での移動体通信端末101と移動体通信経由認証手段322間の回線設定までの手順は、図7の実施の形態2の個人認証手順<手順1>～<手順17>と同様である。

【0080】<手順18>移動体通信事業者400からの回線接続結果が回線接続成功であった場合、移動体通信経由認証手段322は、テスト信号をオープンな情報通信路202を用いてサービス端末101へ送信し、送信したテスト信号を送信テスト信号として記憶する。

【0081】ここで、テスト信号は、乱数等を用いて発生させた任意の信号を用いてもよいし、事前に移動体通信経由認証手段322が記憶している任意の信号を用いてもよい。

【0082】<手順19>サービス端末101は、「サービス端末、移動体通信端末間通信路」203を用いて前記テスト信号を移動体通信端末102へ送信する。

【0083】<手順20>移動体通信端末102は、移動体通信通信路201に設定された回線を用いて前記テスト信号を移動体通信事業者400へ送信する。

【0084】<手順21>移動体通信事業者400は、前記テスト信号を移動体通信経由認証手段322へ送信する。

【0085】<手順22>移動体通信経由認証手段322は、前記テスト信号を受信すると、記憶している「送信テスト信号」と受信したテスト信号を比較照合し、同一であれば、移動体通信経由認証が成立したと判定し、同一でない場合は、移動体通信経由認証が不成立であったと判定する。

【0086】<手順23>移動体通信経由認証手段322は、「会員ID番号」と共に、移動体通信経由認証の認証結果を個人認証管理手段323へ通知する。

【0087】<手順24>個人認証管理手段323は、移動体通信経由認証手段322から送られてきた認証結果が、移動体通信経由認証の成立である場合には、個人認証が成功したと判定し、サービス提供装置300からサービス端末101へのサービス提供を開始する。

【0088】また、認証結果が、移動体通信経由認証が不成立であった場合、個人認証管理手段323はサービス端末101へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【0089】(実施の形態4)本実施の形態の構成は、図9に示す実施の形態2の個人認証システムと同様である。また、本実施の形態で示す個人認証システムを実現するために必要な会員ユーザ情報も図6に示す実施の形

態2の会員情報と同様である。本実施の形態と実施の形態2では、認証手順が異なっており、図9は、本実施の形態で示す個人認証システムの認証手順を示したフローレーション図である。

【0090】ここで、図9の手順1～手順24の数字は、認証手順の順番を示している。以下、本実施の形態で示す個人認証システムの動作を図9の認証手順毎に説明する。

【0091】<手順1>～<手順12>被認証者100のサービス提供要求主から基本認証の成立、移動体通信端末102の呼び出し操作までは、図7の実施の形態2の個人認証手順<手順2>～<手順13>と同様である。

【0092】<手順13>移動体通信事業者400から回線接続要求を受けた移動体通信端末102は、回線接続要求を受けていることを被認証者100に呼び出しベル、バイブレーション等を用いて通知する。

【0093】<手順14>被認証者100は、所持する移動体通信端末102をサービス端末101へ「サービス端末、移動体通信端末間通信路」203を用いて接続する。

【0094】<手順15>被認証者100は、移動体通信端末102に設置されている応答ボタン等を押すことにより回線接続要求に応答する。なお、この応答作業は、手順14の移動体通信端末102とサービス端末101の接続作業により自動的に実施されることとしてもよい。

【0095】<手順16>移動体通信端末102は、応答があったことを移動体通信通信路201を用いて移動体通信事業者400へ通知し、移動体通信通信路201に回線を設定する。

【0096】<手順17>移動体通信事業者400は、回線接続結果を移動体通信経由認証手段322へ通知する。ここで、移動体通信経由認証手段322は、移動体通信事業者400から送付された回線接続結果が、回線接続失敗であった場合、移動体通信経由認証が不成立であったと判定し、手順23へ進む。

【0097】<手順18>移動体通信事業者400からの回線接続結果が回線接続成功であった場合、移動体通信経由認証手段322は、テスト信号を移動体通信事業者400へ送信し、送信したテスト信号を送信テスト信号として記憶する。ここで、テスト信号は、乱数等を用いて発生させた任意の信号を用いてもよいし、事前に移動体通信経由認証手段322が記憶している任意の信号を用いてもよい。

【0098】<手順19>移動体通信事業者400は、移動体通信通信路201に設定された回線を用いて前記テスト信号を移動体通信端末102へ送信する。

【0099】<手順20>移動体通信端末102は、「サービス端末、移動体通信端末間通信路」203を用いて前記テスト信号をサービス端末101へ送信する。

【0100】<手順21>サービス端末101は、オープンな情報通信路202を用いて前記テスト信号を移動体通信経由認証手段322へ送信する。

【0101】<手順22>移動体通信経由認証手段322は、前記テスト信号を受信すると、記憶している「送信テスト信号」と受信したテスト信号を比較照合し、同一であれば、移動体通信経由認証が成立したと判定し、同一でない場合は、移動体通信経由認証が不成立であったと判定する。

【0102】<手順23>移動体通信経由認証手段322は、「会員ID番号」と共に、移動体通信経由認証の認証結果を個人認証管理手段323へ通知する。

【0103】<手順24>個人認証管理手段323は、移動体通信経由認証手段322から送られてきた認証結果が、移動体通信経由認証の成立である場合には、個人認証が成功したと判定し、サービス提供装置300からサービス端末101へのサービス提供を開始する。

【0104】また、認証結果が、移動体通信経由認証が不成立であった場合、個人認証管理手段323はサービス端末101へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【0105】(実施の形態5) 本実施の形態の構成は、図5に示す実施の形態2の個人認証システムと同様である。また、本実施の形態で示す個人認証システムを実現するために必要な会員ユーザ情報も図6に示す実施の形態2の会員情報と同様である。本実施の形態と実施の形態2では、認証手順が異なっており、図10は、本実施の形態で示す個人認証システムの認証手順を示したフローレーション図である。

【0106】ここで、図10の手順1～手順24の数字は、認証手順の順番を示している。以下、本実施の形態で示す個人認証システムの動作を図10の認証手順毎に説明する。

【0107】<手順1>～<手順17>被認証者100のサービス提供要求主から基本認証の成立、移動体通信通信路201上での移動体通信端末101と移動体通信経由認証手段322間の回線設定までの手順は、図9の実施の形態4の個人認証手順<手順1>～<手順17>と同様である。

【0108】<手順18>移動体通信事業者400からの回線接続結果が回線接続成功であった場合、移動体通信経由認証手段322は、テスト信号をオープンな情報通信路202を用いてサービス端末101へ送信し、送信したテスト信号を送信テスト信号として記憶する。

【0109】ここで、テスト信号は、乱数等を用いて発生させた任意の信号を用いてもよいし、事前に移動体通信経由認証手段322が記憶している任意の信号を用いてもよい。

【0110】<手順19>サービス端末101は、「サービス端末、移動体通信端末間通信路」203を用いて前



記テスト信号を移動体通信端末102へ送信する。

【0111】<手順20>移動体通信端末102は、移動体通信通信路201に設定された回線を用いて前記テスト信号を移動体通信事業者400へ送信する。

【0112】<手順21>移動体通信事業者400は、前記テスト信号を移動体通信経由認証手段322へ送信する。

【0113】<手順22>移動体通信経由認証手段322は、前記テスト信号を受信すると、記憶している「送信テスト信号」と受信したテスト信号を比較照合し、同一であれば、移動体通信経由認証が成立したと判定し、同一でない場合は、移動体通信経由認証が不成立であったと判定する。

【0114】<手順23>移動体通信経由認証手段322は、「会員ID番号」と共に、移動体通信経由認証の認証結果を個人認証管理手段323へ通知する。

【0115】<手順24>個人認証管理手段323は、移動体通信経由認証手段322から送られてきた認証結果が、移動体通信経由認証の成立である場合には、個人認証が成功したと判定し、サービス提供装置300からサービス端末101へのサービス提供を開始する。

【0116】また、認証結果が、移動体通信経由認証が不成立であった場合、個人認証管理手段323はサービス端末101へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【0117】(実施の形態6) 図11は、本実施の形態における個人認証システムを応用した自販機等のサービス設備の課金システム、サービスを示す概念図である。図11において、200は、需要者に対しサービス供給と、その供給したサービスに対する課金が可能なサービス提供者が保有するサービス設備、11は、サービス設備200に対してサービス供給を要請し、そのサービスを受受するサービス受給者、12は、サービス受給者11のサービス設備200からのサービス受受の可否決定、並びに、サービス受給者が受受したサービスに対する課金を請け負う課金対象者、300は、サービス設備からの問い合わせに対して、サービス受給者11の個人認証、並びに、課金を実行する課金装置、102は、課金対象者12が所持する課金装置300に事前登録されている移動体通信端末、400は、移動体通信端末102を統括するPNS、携帯電話等の移動体通信事業者、202は、サービス設備200と課金装置300を接続するオープンな情報通信路、201は、移動体通信事業者400と移動体通信端末102を接続する移動体通信通信路である。

【0118】ここで、オープンな情報通信路202とはインターネットなど不特定多数のサービス設備が任意の課金装置へアクセス可能な情報通信路を示しており、このオープンな情報通信路202を用いて接続される課金装置300は、例えば、サービス設備である自販機の物

品販売時のキャッシュレス課金サービス等を提供する。

【0119】なお、図11においては、課金装置300の課金サービスの利用者であるサービス設備200が一台のみ示されているが、一般的应用においては、複数のサービス設備が存在しており、サービス設備200はその内の一台のみを示している。

【0120】また、ここでは、サービス受給者11と課金対象者12を別個なものとしているが、サービス受給者、課金対象者が同一でも良い。

【0121】さらに、ここでは、課金装置300と移動体通信事業者400を別個なものとしているが、課金装置200と移動体通信事業者400は同一であるとしてもよい。

【0122】図12は、本実施の形態における課金装置300の構成を示す概念図である。図12において、310は、サービス受給対象者11、並びに、課金対象者12として事前登録されている会員の会員ユーザ情報を記憶する会員データベース、320は、課金装置300で課金サービス実施可能な事前登録されたサービス設備(施設)の施設情報を記憶する施設データベース、302は、課金サービスを要請するサービス設備200が事前登録されたサービス設備であるか、否かを認証、判断する施設認証手段、303は、サービス設備200へサービス要求を行なっているサービス受給者11が正規の会員か否かをオープンな情報通信路202を用いて認証判断する基本認証手段、305は、サービス受給者11に対応する課金対象者12が所持している移動体通信端末を用いてサービス受給者11のサービス受受可否、および認証を判断する移動体通信経由認証手段、304は、基本認証手段303、及び、移動体通信経由認証手段304の認証結果に基づき課金対象者12に課金をする課金手段、301は、施設認証手段302、基本認証手段303、課金手段304、移動体通信経由認証手段305を統括管理し、個人認証の判断、及び課金を実行する課金認証手段である。

【0123】図13は、本実施の形態で示す個人認証システムを応用した自販機等のサービス設備200の課金システムを実現するために必要な施設情報の例を示しており、この施設情報は、施設データベース320に事前に登録されている。図13には、2つの施設の施設情報が記憶されている例を示しており、1つの施設情報の内訳は、対応する1つの「施設名」、サービス設備200がオープンな情報通信路202経由で施設認証を行う時に用いる1つの「施設ID」と「施設認証パスワード」、並びに、該施設がオープンな情報通信路202上で通信を行うために必要なサービス設備200の「施設アドレス」、該施設で実施可能なサービス種を示す、1から複数の「選択可能サービス名称」、そして、サービス設備200に付帯する設置位置等の「その他情報」である。

【0124】図14は、本実施の形態で示す個人認証シ



システムを応用した自販機等のサービス設備200の課金システムを実現するために必要な会員ユーザ情報の例を示しており、この会員ユーザ情報は、会員データベース310に事前に登録されている。図14には、2名の会員ユーザ情報が記憶されている例を示しており、1つの会員情報の内訳は、対応する1つの「会員氏名」、サービス受給者11がオープンな情報通信路202経由で認証を行う時に用いる1から複数の「会員ID番号」及び「会員ID番号」に対応した同数の「基本認証パスワード情報」、移動体通信通信路201経由で認証、並びに、サービス受給の可否判断を行う時に用いる1つの「移動体通信端末呼び出し番号」、及び1つの「移動体通信経由認証パスワード情報」、課金時の使用可能金額を示す1つの「使用可能金額」、課金記録を示す0から複数の「課金記録」である。

【0125】図15は、本実施の形態における切符券売機、ジュース自販機、煙草自販機等の自動販売機器を想定したサービス設備200の構成例を示す概念図である。図15において、203は、キーボード、ボタン、タッチパネル等、サービス受給者11からの情報を取り込みことが可能な入力部、203は、液晶ディスプレイ、LED表示機、ブラウン管等のサービス設備200の情報をサービス受給者へ表示することが可能な出力部、205は、サービス受給者11が所望した物品をサービス受給者へ供給することが可能な物品送出部、210は、サービス設備200が提供可能な物品の物品情報を記憶する設備管理DB、204は、オープンな情報通信路202を用いて変換している課金装置300との通信を実現する通信手段、201は、出力部202、入力部203、通信手段204、物品送出部205を統括する制御部である。

【0126】図16は、本実施の形態で示す個人認証システムを応用した自販機等のサービス設備200の課金システムを実現するために必要な物品情報の例を示しており、この物品情報は、設備管理DB210に事前に登録されている。図16には、3種の物品情報が記憶されている例を示しており、1つの物品情報の内訳は、対応する1つの「物品名」、及び1つの「課金額」である。

【0127】図17は、本実施の形態で示す個人認証システムを応用した自販機等のサービス設備200の課金システムの物理的配置例を示した図である。図17において、200は、通路構にあるジュース自販機、11は、ジュース自販機200からジュースを購入しようとしているサービス受給者、300は、オープンな情報通信路202を通して、ジュース自販機200と接続し、サービス受給者11からのキャッシュレスでのジュース購入要求に対する個人認証、並びに課金を実施する課金装置、12は、ジュース購入を所望するサービス受給者11の認証証明、並びに、ジュース購入の課金可否を決定する課金対象者、102は、課金装置300からの認

証証明要求、サービス許可を課金対象者12に対して、いつでもどこでも表示、入力することが可能な移動体端末、201は、課金装置300と移動体端末102間とをいつでもどこでも接続可能な移動体通信網、400は、移動体通信網を統括している移動体通信事業者である。

【0128】なお、ここでは、サービス受給者11と課金対象者12を別個なものとしているが、サービス受給者、課金対象者が同一でもよい。

【0129】図18は、本実施の形態で示す個人認証システムを応用した自販機等のサービス設備200の課金システムの個人認証、並びに、課金手順を示したコラボレーション図であり、手順1～手順58の数字は、処理手順の順番を示している。以下、個人認証システムを応用した自販機等のサービス設備200の課金システムの動作を図18に使い説明する。

【0130】<手順1>サービス受給者11は、図15に示す例えばジュースの自販機等のサービス設備200のサービス提供を本発明の実施の形態で示す個人認証システムを応用した課金システムを用いて享受するために、サービス設備200内にある入力部203に対して、例えばお菓子の購入等の「選択サービス」をキャッシュレスで購入する旨を入力し、この入力時に「会員ID」及び「基本認証パスワード」も入力する。ここで、「会員ID」及び「基本認証パスワード」とは、課金対象者12が、課金装置300を運用する課金サービス提供者と課金サービス提供契約を交わした際に、課金サービス提供者から通知されるものであり、通知された前記「会員ID」及び「基本認証パスワード」は、課金サービス提供者が保有する課金装置300内の会員データベース310に課金対象者12、あるいは、サービス受給者11の氏名および課金対象者12の所持する移動体通信端末102の移動体端末呼び出し番号と対応付けられ記憶されているものとする。なお、ここで、キャッシュレス購入を要求しないサービス受給者11は、通常のコイン、紙幣、クレジットカード等によるサービス受給が可能となる。

【0131】<手順2>入力部203は、サービス受給者11から要求されたキャッシュレス購入の要望を「選択サービス」、並びに、「会員ID」及び「基本認証パスワード」と共に制御部201へ報告する。

【0132】<手順3>制御部201は、サービス受給者11からのキャッシュレス購入要望を検知し、課金装置300へのアクセス要求を通信手段204へ命令する。

【0133】<手順4>通信手段204は、事前に記憶している課金装置300の情報通信路202上での「アドレス」を用いて、インターネット等のオープンな情報通信路202を通して、通信手段204が事前に記憶している「施設ID」、「施設認証パスワード」、及び、オープンな情報通信路上での自施設（サービス設備200）アドレスを示す「施設アドレス」を課金装置300

0内の課金認証管理手段301へ送付し、サービス設備200の施設認証、並びにアクセス許可を要求する。ここで、「施設ID」及び「施設認証パスワード」とは、サービス設備200を保有するサービス提供者が、課金装置300を運用する課金サービス提供者とサービス提供契約を交わした際に、課金サービス提供者から通知されるものであり、通知された前記「施設ID」及び「施設認証パスワード」は、課金サービス提供者が保有する課金装置300内の施設データベース320にサービス設備200の施設名称、施設ID、施設認証パスワード、施設アドレス、可能選択サービス、その他情報等と対応付けられ記憶されているものとする。

【0134】また、オープンな情報通信路202を使用して前記「施設ID」及び「施設認証パスワード」を通信する場合、これら情報の不正取得を防止することを目的に通信手段204と課金装置300間では情報の伝達を暗号処理し、通信セキュリティを確保してもよい。

【0135】なお、今回、通信手段204にオープンな情報通信路202上での課金装置300の「アドレス」、並びに、サービス設備200の「施設ID」、「施設認証パスワード」、「施設アドレス」を記憶させることとしているが、課金装置300アドレス、該施設ID、該施設認証パスワード、該施設アドレスを設備管理DB210に記憶させ、課金装置300との通信時に制御部201が課金装置300アドレス、該施設ID、該施設認証パスワード、該施設アドレスを設備管理DB210から読み出し、通信手段204へ課金装置300アドレス、該施設ID、該施設認証パスワード、該施設アドレスを通知するとしてもよい。

【0136】＜手順4＞施設認証、アクセス要求および「施設ID」「施設認証パスワード」「施設アドレス」を受信した課金認証管理手段301は、「施設ID」「施設認証パスワード」「施設アドレス」を施設認証302に送付し、「施設ID」に対応するサービス設備の施設認証を要求する。

【0137】＜手順5＞「施設ID」「施設認証パスワード」を課金認証管理手段301から受け取った施設認証手段302は、施設データベース320に対して、課金認証管理手段301より受け取った「施設ID」に対応する「照合用施設認証パスワード」「照合用施設アドレス」を照会する。

【0138】ここで、「照合用施設認証パスワード」とは、施設データベース320が、記憶している「施設ID」に対応した「施設認証パスワード」を示している。また、「照合用施設アドレス」とは、施設データベース320が、記憶している「施設ID」に対応した「施設アドレス」を示している。

【0139】＜手順7＞施設データベース320は、要求のあった「施設ID」をキーワードに、データベース内の施設情報の検索を実行し、同一の「施設ID」を発見した

場合には、この「施設ID」に対応する「照合用施設認証パスワード」「照合用施設アドレス」を施設認証手段302へ送付する。

【0140】ここで、検索の結果、要求のあった「施設ID」が発見できなかった場合は、施設データベース320は、施設認証手段302へ施設IDがないことを通知する。

【0141】＜手順8＞施設認証手段302は、施設データベース320から「照合用施設認証パスワード」が返送されてくると、前記「照合用施設認証パスワード」とサービス設備200から送付された「施設認証パスワード」を比較照合し、同一であれば、施設認証の第一段階が成立したと判定し、手順9へ進む。同一でない場合は、施設認証が不成立であったと判定し、手順10へ進む。

【0142】ここで、施設データベース320から検索すべき「施設ID」が存在しない旨の通知を受けた場合、施設認証手段302は、施設認証が不成立であったと判定し、手順10へ進む。

【0143】＜手順9＞施設認証手段302は、施設データベース320から返送された「照合用施設アドレス」とサービス設備200から送付された「施設アドレス」を比較照合し、同一であれば、施設認証が成立したと判定し、同一でない場合は、施設認証が不成立であったと判定する。

【0144】＜手順10＞施設認証手段302は、「施設ID」「施設アドレス」と共に、施設認証の判定結果を課金認証管理手段301へ通知する。

【0145】＜手順11＞課金認証管理手段301は、施設認証手段302から受けた認証判定結果に基づき、該サービス設備200のアクセス許可の可否を決定し、可否結果を施設アドレスを用いてサービス設備200内の通信手段204へ送信する。

【0146】＜手順12＞アクセス許可の可否結果を受け取った通信手段204は、可否結果を制御部201へ通知する。

【0147】＜手順13＞アクセス許可が可の場合、制御部201は、設備管理DB210に対して、サービス受給者11が入力したお茶の購入等の「選択サービス」に対応する「課金額」を照会し、手順14へ進む。

【0148】アクセス許可が否の場合、制御部201は、出力部202を通して、サービス受給者11へ、個人認証システムを応用した課金システムでの物品購入ができない旨連絡し、通常のコイン、紙幣、クレジットカード等による物品購入を促し、個人認証システムを応用した課金システムの動作を終了する。

【0149】＜手順14＞設備管理DB210は、要求のあった「選択サービス」をキーワードに、データベース内の物品情報の検索を実行し、同一の「選択サービス」を発見した場合には、この「選択サービス」に対応する

「課金額」を制御部201へ送付する。

【0150】<手順15>制御部201は、「課金額」を受け取ると、通信手段204に対して、サービス受給者11が入力した「会員ID」、「基本認証パスワード」、「選択サービス」、並びに、「課金額」を通知し、課金装置300への課金要求送信の命令を下す。

【0151】<手順16>通信手段204は、制御部201から課金要求送信命令を受けると、オープンな情報通信路202を用いて、「会員ID」、「基本認証パスワード」、「選択サービス」、「課金額」を課金装置300内の課金認証管理手段301へ送付し、サービス受給者11の個人認証、並びに、課金サービスの実施を要求する。ここで、オープンな情報通信路202を使用して前記「会員ID」、「基本認証パスワード」、「選択サービス」、「課金額」を送信する場合、これらの情報の不正取得を防止することを目的に通信手段204と課金装置300間では情報の伝達を暗号処理し、通信セキュリティを確保してもよい。

【0152】<手順17>個人認証、及び課金サービス実施要求を受信した課金認証管理手段301は、「会員ID」、「基本認証パスワード」を基本認証手段303に送付し、「会員ID」に対応するサービス受給者11の個人認証を要求する。

【0153】<手順18>「会員ID」、「基本認証パスワード」を課金認証管理手段301から受けた基本認証手段303は、会員データベース310に対して、課金認証管理手段301より受け取った「会員ID」に対応する「照合用基本認証パスワード情報」を要求する。

【0154】ここで、「照合用基本認証パスワード情報」とは、会員データベース310が、記憶している「会員ID」に対応した「基本認証パスワード情報」を示している。

【0155】<手順19>会員データベース310は、要求のあった「会員ID」をキーワードに、データベース内の会員ユーザ情報の検索を実行し、同一の「会員ID」を発見した場合には、この「会員ID」に対応する「照合用基本認証パスワード」を基本認証手段303へ送付する。

【0156】ここで、検索の結果、要求のあった「会員ID」が発見できなかった場合は、会員データベース310は、基本認証手段303へ会員IDがないことを通知する。

【0157】<手順20>基本認証手段303は、会員データベース310から「照合用基本認証パスワード」が返送されてくると、前記「照合用基本認証パスワード」と「基本認証パスワード」を比較照合し、同一であれば、基本認証が成立したと判定し、同一でない場合は、基本認証が不成立であったと判定する。

【0158】ここで、会員データベース310から検索すべき「会員ID」が存在しない旨の通知を受けた場合、

基本認証手段303は、基本認証が不成立であったと判定する。

【0159】<手順21>基本認証手段303は、「会員ID」と共に、基本認証の判定結果を課金認証管理手段301へ通知する。

【0160】<手順22>課金認証管理手段301は、基本認証手段303から送られてきた認証結果が、基本認証成立である場合には、「会員ID」、「施設名称」、「課金額」、「選択サービス」を移動体通信経由認証手段305へ送付し、移動体通信経由認証を要求する。

【0161】ここで、基本認証手段303から送られてきた基本認証の結果が、基本認証不成立であった場合、課金認証管理手段301は個人認証、並びに課金処理を中止し、<手順48>へ進む。

【0162】<手順23>「会員ID」を課金認証管理手段301から受け取った移動体通信経由認証手段305は、会員データベース310に対して、課金認証管理手段301より受け取った「会員ID」に対応する「照合用移動体通信経由認証パスワード」および「移動体通信端末呼び出し番号」を要求する。

【0163】ここで、「照合用移動体通信経由認証パスワード」とは、会員データベース310が、記憶している「会員ID」に対応した「移動体通信経由認証パスワード」を示している。

【0164】<手順24>会員データベース310は、要求のあった「会員ID」をキーワードに、データベース内の会員ユーザ情報の検索を実行し、同一の「会員ID」を発見した場合には、この「会員ID」に対応する「照合用移動体通信経由認証パスワード」および「移動体通信端末呼び出し番号」を移動体通信経由認証手段305へ送付する。

【0165】なお、検索の結果、要求のあった「会員ID」が発見できなかった場合は、会員データベース310は、移動体通信認証手段305へ会員ID番号が存在しないことを通知する。

【0166】<手順25>移動体通信経由認証手段305は、会員データベース310から「照合用移動体通信経由認証パスワード」および「移動体通信端末呼び出し番号」が返送されてくると、移動体通信事業者400に対して「移動体通信端末呼び出し番号」を使用して移動体通信端末102への回線接続要求を行う。なお、移動体通信経由認証手段305が、会員データベース310から検索すべき「会員ID」が存在しない旨の通知を受けた場合、移動体通信手段322は、基本認証が不成立であったと判定し、<手順38>へ進む。

【0167】また、移動体通信経由認証手段305から移動体通信事業者400へ回線接続要求を送信する際使用する通信路は、専用回線あるいは、電気通信網等の公共回線のどちらを使用しても良い。

【0168】<手順26>～<手順15>手順26、手順2

7、手順28、手順29の操作は、移動体通信事業者400の回線接続方法により異なるが、以下、携帯電話等の一般的回線接続方法を示す。

【0169】<手順26>移動体通信事業者400は、移動体通信通信路201を用いて移動体通信端末102に対して回線接続要求を行う。ここで、移動体通信端末102が他の通信に使用されている等で回線接続が不可能である場合は、移動体通信事業者400は、回線接続失敗と判定し、<手順30>へ進む。

【0170】<手順27>移動体通信事業者400から回線接続要求を受けた移動体通信端末102は、回線接続要求を受けていることを課金対象者12に呼び出しベル、バイブレーション等を用いて通知する。

【0171】<手順28>課金対象者12は、移動体通信端末102に設置されている応答ボタン等を押すことにより回線接続要求に応答する。

【0172】<手順29>移動体通信端末102は、課金対象者12から応答があったことを移動体通信通信路201を用いて移動体通信事業者400へ通知し、移動体通信通信路201に回線を設定する。

【0173】<手順30>移動体通信事業者400は、回線接続結果を移動体通信経由認証手段305へ通知する。ここで、移動体通信経由認証手段305は、移動体通信事業者400から送付された回線接続結果が、回線接続失敗であった場合、移動体通信経由認証が不成立であったと判定し、<手順38>へ進む。

【0174】<手順31>～<手順33>

移動体通信事業者400からの回線接続結果が回線接続成功であった場合、移動体通信経由認証手段305は、移動体通信通信路201に設定された回線を用いて、課金対象者12に対して「会員ID」、「施設名称」、「課金金額」、「選択サービス」を提示し、サービス受給者11の個人認証、並びに、該サービス受給に対する許可決定問い合わせとして、「移動体通信経由認証パスワード」の入力を課金対象者12へ要求する。

【0175】ここで、「移動体通信経由認証パスワード」とは、課金対象者12が課金サービス運営者と課金サービス提供契約を交わした際に、サービス提供者から通知されるものであり、通知された前記「移動体通信経由認証パスワード」は、課金サービス運営者が保有する課金装置300内の会員データベース310に課金対象者12の氏名および課金対象者12の所持する移動体通信端末102の移動体端末呼び出し番号等と対応付けられ記憶されているものとする。

【0176】<手順34>～<手順36>

課金対象者12が、「移動体通信経由認証パスワード」を移動体通信端末102へ入力すると、移動体通信端末102は、移動体通信通信路201に設定された回線を用いて「移動体通信経由認証パスワード」を移動体通信経由認証手段305へ送付する。

【0177】<手順37>移動体通信経由認証手段305は、「移動体通信経由認証パスワード」が返送されてくると、前記「照合用移動体通信経由認証パスワード情報」と「移動体通信経由認証パスワード」を比較照合し、同一であれば、移動体通信経由認証が成立したと判定し、同一でない場合は、移動体通信経由認証が不成立であったと判定する。

【0178】<手順38>移動体通信経由認証手段305は、「会員ID」と共に、移動体通信経由認証の認証結果を課金認証管理手段301へ通知する。

【0179】<手順39>課金認証管理手段301は、移動体通信経由認証手段305から送られてきた認証結果が、移動体通信経由認証の成立である場合には、サービス受給者11の個人認証成功、並びに、課金対象者12の課金許可受理と判定する。

【0180】また、認証結果が、移動体通信経由認証が不成立であった場合、課金認証管理手段301は課金処理を中止し、<手順48>に進む。

【0181】<手順40>課金対象者12から課金許可を受領した課金認証手段301は、「施設名称」、「課金金額」、「会員ID」、「選択サービス」を課金手段304に送付し、課金処理を要求する。

【0182】<手順41>課金手段304は、会員データベース310に対して、課金認証管理手段301より受け取った「会員ID」に対応する「会員使用可能金額」を要求する。

【0183】ここで、「会員使用可能金額」とは、会員データベース310が記憶している「会員ID」に対応した「会員使用可能金額」を示している。

【0184】<手順42>会員データベース310は、要求のあった「会員ID」をキーワードに、データベース内の会員ユーザ情報の検索を実行し、同一の「会員ID」を発見した場合には、この「会員ID」に対応する「会員使用可能金額」を課金手段304へ送付する。

【0185】<手順43>課金手段304は、会員データベース310から「会員使用可能金額」が返送されてくると、課金認証管理手段301から送付された「課金額」と「会員使用可能金額」を比較し、例えば「課金額」に対して「会員使用可能金額」が大きいか同一、あるいは、「課金額」と「課金手数料」等の総和に対して「会員使用可能金額」が大きいか同一の場合に課金処理可能と判定し課金処理を開始する（手順44へ進む）。

【0186】ここで、例えば、「課金額」に対して「会員使用可能金額」が小さい、あるいは、「課金額」と「課金手数料」等の総和に対して「会員使用可能金額」が小さい場合等には、課金処理不可と判定し、課金処理を中止し手順46へ進む。

【0187】<手順44>課金手段304は、会員データベース310に対して課金認証管理手段301より受け取った「会員ID」に対応する「会員使用可能金額」項

目、並びに課金記録項目に対して「課金処理後の会員使用可能金額の書換え」「課金記録の追加書き込み」を要求する。ここで、「課金処理後の会員使用可能金額」とは、例えば、会員使用可能金額から課金額を差し引いた金額、あるいは、会員使用可能金額から課金額、並びに、手数料等を差し引いた金額等を示す。

【0188】<手順45>会員データベース310は、要求のあった「会員ID」をキーワードに、データベース内の会員ユーザ情報の検索を実行し、同一の「会員ID」を発見した場合には、この「会員ID」に対応する「会員使用可能金額」項目、並びに「課金記録」項目に対して「課金処理後の会員使用可能金額の書換え」「課金記録の追加書き込み」を実行し、書換え、書き込み処理結果を課金処理手段304へ送付する。

【0189】なお、課金対象者12の課金決済については、課金対象者12が課金装置300を運用する課金サービス提供者と課金サービス提供契約を交わした際に指定した決済口座から、課金装置300が、会員データベース310に記録された課金記録に基づき、例えば、ある一定期間毎、あるいは、リアルタイムに引き落とすとしても良い。また、課金サービス提供者が運営する課金装置300自体が決済機能を持っている場合ならば、会員データベース310を決済口座とし、会員IDに対応する会員使用可能金額を決済口座残高としても良い。この場合、手順44、手順45で示す課金処理が決済処理として機能する。

【0190】また、サービス設備200を運営するサービス提供者と課金装置300間の課金決済については、サービス提供者が課金装置300を運用する課金サービス提供者と課金サービス提供契約を交わした際に指定した決済口座へ、課金装置300が、会員データベース310に記録された課金記録に基づき、例えば、ある一定期間毎、あるいは、リアルタイムに振込むとしても良い。

【0191】また、課金サービス提供者が運営する課金装置300自体が決済機能を持っている場合ならば、施設データベース320内の施設情報に施設IDに対応する「施設使用料金額」項目を追加、各施設の決済口座とし、サービス設備200に対する課金対象者12への課金額を、ある一定期間ごとにとまとめて、あるいは、リアルタイムに該決済口座へ移行するようデータ書換を実施するとしても良い。

【0192】<手順46>課金処理手段301は、会員データベース310から書換え結果を受け取ると、書き込み結果が正常であった場合には、課金処理が正常終了したと判定する。また、書き込み結果が異常であった場合、または、手順43において課金処理不可と判定した場合には、課金処理異常終了と判定する。

【0193】<手順47>課金手段304は、課金処理結果を課金認証管理手段301へ送付する。ここで、課金

手段304から課金処理判定結果を受け取った課金認証管理手段301は、手順48～手順54、手順55～手順58の2つの手順を並行して実行する。

【0194】<手順48>課金処理手段304から課金処理判定結果を受け取った課金認証管理手段301は、課金処理結果を施設アドレスを用いてサービス設備200内の通信手段204へ送信する。

【0195】<手順49>課金認証管理手段301から課金処理結果を受信した通信手段204は、課金処理結果を制御部201へ通知する。

【0196】<手順50>制御部201は、出力部202に課金処理結果に基づくサービス受給可否、並びに、課金額をサービス受給者11へ伝達するよう要求する。

【0197】<手順51、手順52>出力部202は、制御部201から受けた要求に従い、課金処理結果が課金処理正常終了であった場合、「課金処理が正常終了表示」「課金額表示」をサービス受給者11へ示し、手順52へ進む。

【0198】ここで、課金処理結果が課金処理異常終了であった場合、出力部202は、サービス受給者11へ、個人認証システムを応用した課金システムでの物品購入ができない旨連絡し、通常のコイン、紙幣、クレジットカード等による物品購入を促し、個人認証システムを応用した課金システムの動作を終了する。

【0199】<手順53>制御部201は、課金処理結果が課金正常終了であった場合、物品送出部205へサービス受給者11が所望する物品の送出を命令する。

【0200】<手順54>制御部201に基づき、物品送出部205はサービス受給者11が所望する物品を送出し、個人認証システムを応用した課金システムの動作を終了する。

【0201】<手順55>課金処理手段304から課金処理判定結果を受け取った課金認証管理手段301は、「課金処理結果」「施設名称」「課金金額」を課金対象者12へ通知するよう移動体通信経路認証手段305へ要求する。

【0202】<手順56>～<手順58>

移動体通信経路認証手段305は、課金対象者12向けに移動体通信経路201に設定された回線を用いて、課金対象者12に対して「課金処理結果」「施設名称」「課金金額」を提示する。

【0203】(実施の形態7)本実施の形態で示す個人認証システムを応用した定額有料施設、定額駐車場等の課金システムの構成概要、課金装置の構成、課金装置内のある施設データベース、会員データベースは、図11、図12、図13、図14に示す実施の形態6と同様である。本実施の形態と実施の形態6では、図11におけるサービス設備200の構成と配置方法、並びに、サービス受給者11へのサービス受給方法が異なる。

【0204】図19は、本実施の形態における定額有料



施設、定額駐車場等を想定したサービス設備200の構成例を示す概略図である。図19において、203は、キーボード、ボタン、タッチパネル等、サービス受給者11からの情報を取り込みことが可能な入力部。202は、液晶ディスプレイ、LED表示機、ブラウン管等のサービス設備200の情報をサービス受給者へ表示することが可能な出力部。206は、対価を支払ったサービス受給者11にのみ施設入場を許可する入場許可ゲート。210は、料金徴収サービス設備200が提供可能なサービス情報を記憶する設備管理DB。204は、オープンな情報通信路202を用いて登録している課金装置300との通信を実現する通信手段。201は、出力部202、入力部203、通信手段204、入場許可ゲート206を統括する制御部である。

【0205】図20は、本実施の形態における定額有料施設、定額駐車場等を想定したサービス設備200の課金システムを実現するために必要なサービス情報の例を示しており、このサービス情報は、設備管理DB210に事前に登録されている。図20には、4種のサービス情報が記憶されている例を示しており、1つのサービス情報の内訳は、対応する1つの「サービス名」、及び1つの「課金額」である。

【0206】図21は、本実施の形態における定額有料施設、定額駐車場等を想定したサービス設備200の課金システムの物理的配置例を示した図である。図21において、サービス設備200は、有料施設内にある入力部203、出力部202と有料施設内に設置される制御部201、設備管理DB210、通信手段204、有料施設入口に設置される入場許可ゲート206から構成されている。また、図21において、11は、有料施設施設への入場を希望しているサービス受給者、300は、オープンな情報通信路202を通して、サービス設備200と接続し、サービス受給者11からのキャッシュレスでの有料施設への入場要求に対する個人認証、並びに課金を実施する課金装置、12は、有料施設入場を希望するサービス受給者11の認証証明、並びに、入場に対する課金可否を決定する課金対象者、102は、課金装置300からの認証証明要求、サービス許可を課金対象者12に対して、いつでもどこでも表示、入力することが可能な移動体端末、201は、課金装置300と移動体端末102間とをいつでもどこでも接続可能な移動体通信網、400は、移動体通信網を統括している移動体通信事業者である。

【0207】なお、ここでは、サービス受給者11と課金対象者12を別個なものとしているが、サービス受給者、課金対象者が同一でも良い。

【0208】図22は、本実施の形態における定額有料施設、定額駐車場等を想定したサービス設備200の課金システムの個人認証、並びに、課金手順を示したフローチャート図であり、手順1～手順57の数字は、処

理手順の順番を示している。以下、個人認証システムを応用した定額有料施設、定額駐車場等のサービス設備200の課金システムの動作を図23に従い説明する。

【0209】〈手順1〉～〈手順49〉

サービス受給者11のサービス設備のサービス選択、並びに、図21に示す例えば有料施設等のサービス設備200の入場料支払いを本発明の実施の形態で示す個人認証システムを応用した課金システムを用いて享受するための、個人認証手順、課金処理手順は、実施の形態6の手順1～手順49と同様である。

【0210】〈手順50〉制御部201は、出力部202に課金処理結果に基づくサービス受給可否、並びに、課金額をサービス受給者11へ伝達するよう要求する。

【0211】〈手順51、手順52〉出力部202は、制御部201から受けた要求に従い、課金処理結果が課金処理正常終了であった場合、「課金処理が正常終了表示」「課金額表示」をサービス受給者11へ示し、手順53へ進む。

【0212】ここで、課金処理結果が課金処理異常終了であった場合、出力部202は、サービス受給者11へ、個人認証システムを応用した課金システムでの入場ができない旨連絡し、通常のコイン、紙幣、クレジットカード等による入場料支払いを促し、個人認証システムを応用した課金システムの動作を終了する。

【0213】〈手順53〉制御部201は、課金処理結果が課金正常終了であった場合、入場許可ゲート206へサービス受給者11への入場許可を命令する。

【0214】〈手順54〉課金処理手段304から課金処理判定結果を受け取った課金認証管理手段301は、「課金処理結果」「施設名称」「課金金額」を課金対象者12へ通知するよう移動体通信経由認証手段305へ要求する。

【0215】〈手順56〉～〈手順58〉

移動体通信経由認証手段305は、課金対象者12向けに移動体通信通信路201に設定された暗鍵を用いて、課金対象者12に対して「課金処理結果」「施設名称」「課金金額」を提示する。

【0216】〈実施の形態8〉本実施の形態で示す個人認証システムを応用した時間制の有料施設、駐車場等の課金システムの構成概要、課金装置の構成、課金装置内のある施設データベース、会員データベースは、図11、図12、図13、図14に示す実施の形態6と同様である。

【0217】本実施の形態と実施の形態6では、図11におけるサービス設備200の構成と配置方法、並びに、課金システムの動作手順が異なる。特に、定額課金の課金システムを示した実施の形態6、並びに、実施の形態7では一連の課金動作（トランザクション）は一回で終了するのに対して、時間制課金を示す本実施の形態では、入場時の個人認証、課金可否確認動作（入場トラ



ンザクション)と出場時の個人認証、課金動作(出場トランザクション)の2回のトランザクションに分けて課金動作を実施する。

【0218】図23は、本実施の形態における時間制の有料施設、駐車場等を想定したサービス設備200の構成例を示す概念図である。図23において、203aは、キーボード、ボタン、タッチパネル等、入場時のサービス受給者11からの情報を取り込みことが可能な入場申請入力部。202aは、液晶ディスプレイ、LED表示機、ブラウン管等のサービス設備200の情報を入場時のサービス受給者へ表示することが可能な入場申請出力部。203bは、キーボード、ボタン、タッチパネル等、出場時のサービス受給者11からの情報を取り込みことが可能な出場申請入力部。202bは、液晶ディスプレイ、LED表示機、ブラウン管等のサービス設備200の情報を出場時のサービス受給者へ表示することが可能な出場申請出力部。206aは、課金可能なサービス受給者11にのみ施設入場を許可する入場許可ゲート。206bは、課金可能なサービス受給者11にのみ施設出場を許可する出場許可ゲート。210は、料金徴収サービス設備200が提供可能なサービス情報を記憶する設備管理DB。204は、オープンな情報通信路202を用いて登録している課金装置300との通信を実現する通信手段。201は、入場申請出力部202a、入場申請入力部203a、出場申請出力部202b、出場申請入力部203b、通信手段204、入場許可ゲート206a、出場許可ゲート206bを統括する制御部である。

【0219】図24は、本実施の形態における時間制の有料施設、駐車場等を想定したサービス設備200の課金システムを実現するために必要なサービス情報の例を示しており、このサービス情報は、設備管理DB210に事前に登録されている。図24には、二人、或いは、3名のサービス情報が記憶されている例を示しており、1つのサービス情報の内訳は、入場者一人一人(あるいは、入場車両一台一台)に対応する「会員ID」、並びに「会員ID」に対応する1つの「入場時刻」「現在時刻での課金金額」「課金情報」である。

【0220】図25は、本実施の形態における時間制有料施設、駐車場等を想定したサービス設備200の課金システムの物理的配置例を示した図である。図25において、サービス設備200は、有料施設入口前にある入場申請入力部203a、入場申請出力部202aと有料施設出口前にある出場申請入力部203b、出場申請出力部202bと有料施設内に設置される制御部201、設備管理DB210、通信手段204、有料施設入口に設置される入場許可ゲート206a、有料施設出口に設置される出場許可ゲート206bから構成されている。また、図25において、11は、有料施設への入場、出場を希望しているサービス受給者。300は、オープン

な情報通信路202を通して、サービス設備200と接続し、サービス受給者11からのキャッシュレスでの有料施設への入場要求に対する個人認証、並びに課金を実施する課金装置。12は、有料施設入出場を所望するサービス受給者11の認証証明、並びに、出場に対する課金可否を決定する課金対象者。102は、課金装置300からの認証証明要求。サービス許可を課金対象者12に対して、いつでもどこでも表示、入力することが可能な移動体端末。201は、課金装置300と移動体端末102間をいつでもどこでも接続可能な移動体通信網。400は、移動体通信網を統括している移動体通信事業者である。

【0221】なお、ここでは、サービス受給者11と課金対象者12を別個なものとしているが、サービス受給者、課金対象者が同一でも良い。

【0222】図26は、本実施の形態における時間制有料施設、駐車場等を想定したサービス設備200の課金システムの入場トランザクション(個人認証、並びに、課金可否)を示したフローチャート図であり、手順1～手順43の数字は、処理手順の順番を示している。以下、個人認証システムを応用した時間制有料施設、駐車場等のサービス設備200の課金システムの動作を図26に従い説明する。

【0223】<手順1>～<手順12>サービス受給者11のサービス要求からサービス設備200の課金装置300へのアクセス可否受信までの施設認証等の手順は、実施の形態6の手順1～手順12と同様である。

【0224】<手順13>通信手段204からアクセス許可が可の場合、制御部201は、通信手段204に対して、サービス受給者11が入力した「会員ID」「基本認証パスワード」を通知し、課金装置300への課金可否問い合わせ要求送信の命令を下す。

【0225】アクセス許可が否の場合、制御部201は、出力部202を通して、サービス受給者11へ、個人認証システムを応用した課金システムでの課金処理ができない旨連絡し、入場券の発行等による通常の入場を促し、個人認証システムを応用した課金システムの動作を終了する。

【0226】<手順14>通信手段204は、制御部201から課金要求送信命令を受けると、オープンな情報通信路202を用いて、「会員ID」「基本認証パスワード」を課金装置300内の課金認証管理手段301へ送付し、サービス受給者11の個人認証、並びに、課金可否問い合わせの実施を要求する。ここで、オープンな情報通信路202を使用して前記「会員ID」「基本認証パスワード」を通信する場合、これら情報の不正取得を防止することを目的に通信手段204と課金装置300間では情報の伝達を暗号処理し、通信セキュリティを確保してもよい。

【0227】<手順15>個人認証、及び課金可否問い合わせ

わせ実施要求を受信した課金認証管理手段301は、「会員ID」「基本認証パスワード」を基本認証手段303に送付し、「会員ID」に対応するサービス受給者11の個人認証を要求する。

【0228】<手順16>〜<手順18>

基本認証手段303の基本認証手順は、実施の形態6の手順18〜手順20と同様である。

【0229】<手順19>基本認証手段303は、「会員ID」と共に、基本認証の判定結果を課金認証管理手段301へ通知する。

【0230】<手順20>課金認証管理手段301は、基本認証手段303から送られてきた認証結果が、基本認証成立である場合には、「会員ID」「施設名称」を移動体通信経由認証手段305へ送付し、移動体通信経由認証を要求する。

【0231】ここで、基本認証手段303から送られてきた基本認証の結果が、基本認証不成立であった場合、課金認証管理手段301は個人認証を中止し、<手順37>へ進む。

【0232】<手順21>〜<手順35>

移動体通信経由認証手段305の移動体通信経由認証手順は、実施の形態6の手順23〜手順37と同様である。

【0233】<手順36>移動体通信経由認証手段305は、「会員ID」と共に、移動体通信経由認証の認証結果を課金認証管理手段301へ通知する。

【0234】<手順37>課金認証管理手段301は、移動体通信経由認証手段305から送られてきた認証結果が、移動体通信経由認証の成立である場合には、サービス受給者11の個人認証成功、並びに、課金対象者12の課金許可と判定する。

【0235】また、認証結果が、移動体通信経由認証が不成立であった場合、課金認証管理手段301は個人認証失敗、課金不可と判定する。

【0236】<手順38>管理手段301は、課金可否結果を施設アドレスを用いてサービス設備200内の通信手段204へ送信する。

【0237】<手順39>課金認証管理手段301から課金可否結果を受信した通信手段204は、課金可否結果を制御部201へ通知する。

【0238】<手順40>制御部201は、入場申請出力部202aに課金可否結果に基づくサービス受給可否、並びに、をサービス受給者11へ伝達するよう要求する。

【0239】<手順41>入場申請出力部202aは、制御部201から受けた要求に従い、課金可否結果が課金許可であった場合、「課金許可表示」をサービス受給者11へ示し手順42へ進む。

【0240】ここで、課金可否結果が課金不可であった場合、入場申請出力部202aは、サービス受給者11

へ個人認証システムを応用した課金システムでの課金処理ができない旨連絡し、入場券の発行等による通常の入場を促し、個人認証システムを応用した課金システムの動作を終了する。

【0241】<手順42>制御部201は、課金可否結果が課金許可であった場合、入場許可ゲート206aへサービス受給者11への入場許可を命令する。

【0242】<手順43>制御部201は、課金可否結果が課金許可であった場合、サービス受給者11の会員IDと共に、入場時刻を設備管理DB210へ記録する。

【0243】図27は、本実施の形態における時間制有料施設、駐車場等を想定したサービス設備200の課金システムの出場ランザクション（個人認証、並びに、課金処理）を示したコラガレーション図であり、手順1〜手順58の数字は、処理手順の順番を示している。以下、個人認証システムを応用した時間制有料施設、駐車場等のサービス設備200の課金システムの動作を図27に使い説明する。

【0244】<手順1>〜<手順12>サービス受給者11の出場要求入力からサービス設備200の課金装置300へのアクセス可否受信までの施設認証等の手順は、実施の形態6の手順1〜手順12と同様である。

【0245】<手順13>アクセス許可が可の場合、制御部201は、設備管理DB210に対して、サービス受給者11の「会員ID」に対応する入場時刻を要求し、手順14へ進む。

【0246】アクセス許可が否の場合、制御部201は、出力部202を通して、サービス受給者11へ、個人認証システムを応用した課金システムでの有料施設使用料金支払いができない旨と、支払い金額を連絡し、通常のコイン、紙幣、クレジットカード等による使用料支払いを促し、個人認証システムを応用した課金システムの動作を終了する。

【0247】<手順14>設備管理DB210は、要求のあった「会員ID」をキーワードに、データベース内のサービス情報の検索を実行し、同一の「会員ID」を発見した場合には、この「会員ID」に対応する「入場時刻」を制御部201へ送付する。

【0248】<手順15>制御部201は、「入場時刻」を受け取ると、現在時刻との差分からサービス受給者11の施設使用料金（課金額）を算出する。

【0249】<手順16>〜<手順50>

サービス受給者11のサービス設備のサービス選択、並びに、有料施設等のサービス設備200の使用料金支払いを本発明の実施の形態で示す個人認証システムを応用した課金システムを用いて享受するための、個人認証手順、課金処理手順は、実施の形態6の手順15〜手順49と同様である。

【0250】<手順51>制御部201は、出場申請出力部202bに課金処理結果に基づくサービス受給可否、

並びに、課金額をサービス受給者11へ伝達するよう要求する。

【0251】<手順52、手順53>出場申請出力部2026は、制御部201から受けた要求に従い、課金処理結果が課金処理正常終了であった場合、「課金処理が正常終了表示」「課金額表示」をサービス受給者11へ示し、手順54へ進む。

【0252】ここで、課金処理結果が課金処理異常終了であった場合、出場申請出力部2026は、サービス受給者11へ、個人認証システムを応用した課金システムでの有料施設使用料金支払いができない旨連絡し、通常のコイン、紙幣、クレジットカード等による使用料金支払いを促し、個人認証システムを応用した課金システムの動作を終了する。

【0253】<手順54>制御部201は、課金処理結果が課金正常終了であった場合、出場許可ゲート2065へサービス受給者11への出場許可を命令する。

【0254】<手順55>課金処理手段304から課金処理判定結果を受け取った課金認証管理手段301は、「課金処理結果」「施設名称」「課金金額」を課金対象者12へ通知するよう移動体通信経由認証手段305へ要求する。

【0255】<手順56>～<手順58>

移動体通信経由認証手段305は、課金対象者12向けに移動体通信通信路201に設定された回線を用いて、課金対象者12に対して「課金処理結果」「施設名称」「課金金額」を提示する。

【0256】(実施の形態9) 本実施の形態で示す個人認証システムを応用した自販機等の課金システムの構成概要は実施の形態6の図11と同様であり、サービス設備200の構成、サービス設備200内における設備管理部、並びに課金システムの物理的配置も実施の形態6の図15、図16、並びに図17と同様である。本実施の形態と実施の形態6では、図11における課金装置300の構成とサービス受給者11へのサービス受給方法が異なる。図28は、本実施の形態における課金装置300の構成を示す概念図である。図28において、310は、サービス受給対象者11、並びに、課金対象者12として事前登録されている会員の会員ユーザ情報を記憶する会員データベース、303は、サービス設備200へサービス要求を行なっているサービス受給者11が正規の会員か否かをオープンな情報通信路202を用いて認証判断する基本認証手段、305は、サービス受給者11に対応する課金対象者12が所持している移動体通信端末を用いてサービス受給者11のサービス享受可否、および認証を判断する移動体通信経由認証手段、304は、基本認証手段303、及び、移動体通信経由認証手段304の認証結果に基づき課金対象者12に課金決済、振込みを実施する課金手段、301は、施設認証手段302、基本認証手段303、課金手段304、移

動体通信経由認証手段305を統括管理し、個人認証の判断、及び課金を実行する課金認証手段である。

【0257】図29は、本実施の形態で示す個人認証システムを応用した自販機等のサービス設備200の課金システムを実現するために必要な会員ユーザ情報の例を示しており、この会員ユーザ情報は、会員データベース310に事前に登録されている。

【0258】図29には、2名の会員ユーザ情報が記憶されている例を示しており、1つの会員情報の内訳は、対応する1つの「会員氏名」、サービス受給者11がオープンな情報通信路202経由で認証を行う時に用いる1から複数の「会員ID番号」及び「会員ID番号」に対応した同数の「基本認証パスワード情報」、移動体通信通信路201経由で認証、並びに、サービス受給の可否判断を行う時に用いる1つの「移動体通信端末呼び出し番号」、及び1つの「移動体通信経由認証パスワード情報」、課金時の使用可能金額を示す1つの「使用可能金額」、決済記録を示す0から複数の「決済記録」である。

【0259】実施の形態6の課金装置300では、図12の課金装置構成、並びに図18のコラボレーション図に示すとおり、課金動作において図12の施設認証手段302、施設データベース320を用いて、課金装置300とサービス設備200間での事前契約の確認をしている。このため、サービス受給者11は、自分が加入、会員登録している課金装置300と事前契約しているサービス設備200に対してしか本発明で示す個人認証システムを応用した課金システムサービスを受受することができない。

【0260】これに対して本実施の形態の課金装置は、サービス受給者11がオープンな情報通信路202に接続されるサービス設備200であれば、サービス設備200と課金装置300間の契約関係にかかわることなく、本発明で示す個人認証システムを応用した課金システムサービスを受受することが可能となる。

【0261】図30は、本実施の形態で示す個人認証システムを応用した自販機等のサービス設備200の課金システムの個人認証、並びに、課金手順を示したコラボレーション図であり、手順1～手順48の数字は、処理手順の順番を示している。以下、個人認証システムを応用した自販機等のサービス設備200の課金システムの動作を図30に言い説明する。

【0262】<手順1>サービス受給者11は、図30に示す例えばジュースの自販機等のサービス設備200のサービス提供を本発明の実施の形態で示す個人認証システムを応用した課金システムを用いて享受するために、サービス設備200内にある入力部203に対して、例えばお金の投入等の「選択サービス」をキャッシュレスで投入する旨入力し、この入力時に「会員ID」「基本認証パスワード」及び「課金装置のオープンな情報通信路

202上のアドレス（以後、課金装置のアドレス）」も入力する。

【0263】ここで、「会員ID」及び「基本認証パスワード」とは、課金対象者12が、課金装置300を運用する課金サービス提供者と課金サービス提供契約を交わした際に、課金サービス提供者から通知されるものであり、通知された前記「会員ID」及び「基本認証パスワード」は、課金サービス提供者が保有する課金装置300内の会員データベース310に課金対象者12、あるいは、サービス受給者11の氏名および課金対象者12の所持する移動体通信端末102の移動体端末呼び出し番号と対応付けられ記憶されているものとする。

【0264】なお、ここで、キャッシュレス購入を要求しないサービス受給者11は、通常のコイン、紙幣、クレジットカード等によるサービス受給が可能となる。

【0265】<手順2>入力部203は、サービス受給者11から要求されたキャッシュレス購入の要望を「選択サービス」、並びに、「会員ID」「基本認証パスワード」および「課金装置300のアドレス」と共に制御部201へ報告する。

【0266】<手順3>制御部201は、サービス受給者11からのキャッシュレス購入要望を検知し、設備管理DB210に対して、サービス受給者11が入力したお茶の購入等の「選択サービス」に対応する「課金額」を要求する。

【0267】<手順4>設備管理DB210は、要求のあった「選択サービス」をキーワードに、データベース内の物品情報の検索を実行し、同一の「選択サービス」を発見した場合には、この「選択サービス」に対応する「課金額」を制御部201へ送付する。

【0268】<手順5>制御部201は、「課金額」を受け取ると、通信手段204に対して、サービス受給者11が入力した「会員ID」「基本認証パスワード」「選択サービス」「課金額」「課金装置300のアドレス」を通知し、課金装置300への課金要求送信の命令を下す。

【0269】<手順6>通信手段204は、制御部201から課金要求送信命令を受けると、オープンな情報通信路202を用いて、「会員ID」「基本認証パスワード」「選択サービス」「課金額」「サービス設備200のオープンな情報通信路202上のアドレス（以後、サービス設備アドレス）」「サービス設備200の施設名称」「サービス設備200の搬送先口座番号」を課金装置300内の課金認証管理手段301へ送付し、サービス受給者11の個人認証、並びに、課金決済（口座振込）サービスの実施を要求する。

【0270】ここで、オープンな情報通信路202を使用して前記「会員ID」「基本認証パスワード」「選択サービス」「課金額」「サービス設備200アドレス」「サービス設備200の施設名称」「サービス設備200の搬送先口座番号」を通信する場合、これらの情報の不正取得を防止することを目的に通信手段204と課金装置300間では情報の伝達を暗号処理し、通信セキュリティを確保してもよい。

【0271】<手順7>個人認証、及び課金決済実施要求を受信した課金認証管理手段301は、「会員ID」「基本認証パスワード」を基本認証手段303に送付し、「会員ID」に対応するサービス受給者11の個人認証を要求する。

【0272】<手順8>～<手順10>基本認証手段303の基本認証手順は、実施の形態6の手順18～手順20と同様である。

【0273】<手順11>基本認証手段303は、「会員ID」と共に、基本認証の判定結果を課金認証管理手段301へ通知する。

【0274】<手順12>課金認証管理手段301は、基本認証手段303から送られてきた認証結果が、基本認証成立である場合には、「会員ID」「施設名称」を移動体通信経由認証手段305へ送付し、移動体通信経由認証を要求する。

【0275】ここで、基本認証手段303から送られてきた基本認証の結果が、基本認証不成立であった場合、課金認証管理手段301は個人認証、を中止し、<手順29>へ進む。

【0276】<手順13>～<手順27>移動体通信経由認証手段305の移動体通信経由認証手順は、実施の形態6の手順23～手順37と同様である。

【0277】<手順28>移動体通信経由認証手段305は、「会員ID」と共に、移動体通信経由認証の認証結果を課金認証管理手段301へ通知する。

【0278】<手順29>課金認証管理手段301は、移動体通信経由認証手段305から送られてきた認証結果が、移動体通信経由認証の成立である場合には、サービス受給者11の個人認証成功、並びに、課金対象者12の課金許可と判定する。

【0279】また、認証結果が、移動体通信経由認証が不成立であった場合、課金認証管理手段301は課金処理を中止し、<手順38>に進む。

【0280】<手順30>課金対象者12から課金許可を受領した課金認証手段301は、「サービス設備200の施設名称」「課金金額」「会員ID」「選択サービス」「サービス設備200の搬送先口座番号」を課金手段304に送付し、課金決済処理を要求する。

【0281】<手順31>課金手段304は、会員データベース310に対して、課金認証管理手段301より受け取った「会員ID」に対応する「会員使用可能金額」を要求する。

【0282】ここで、「会員使用可能金額」とは、会員データベース310が記憶している「会員ID」に対応

した「会員使用可能金額」を示している。

【0283】<手順32>会員データベース310は、要求のあった「会員ID」をキーワードに、データベース内の会員ユーザ情報の検索を実行し、同一の「会員ID」を発見した場合には、この「会員ID」に対応する「会員使用可能金額」を課金手段304へ送付する。

【0284】<手順33、手順34>課金手段304は、会員データベース310から「会員使用可能金額」が返送されてくると、課金認証管理手段301から送付された「課金額」と「会員使用可能金額」を比較し、例えば「課金額」に対して「会員使用可能金額」が大きいか同一、あるいは、「課金額」と「課金決済手数料」等の総和に対して「会員使用可能金額」が大きいか同一の場合にサービス設備200への振込み処理可能と判定し、サービス受給者11から送付された「サービス設備200の振込先口座番号」に対して、「課金額」の振込み作業を実施し、手順34へ進む。

【0285】ここで、例えば、「課金額」に対して「会員使用可能金額」が小さい、あるいは、「課金額」と「課金手数料」等の総和に対して「会員使用可能金額」が小さい場合等には、課金処理不可と判定し、課金処理を中止し手順37へ進む。

【0286】<手順35>課金手段304は、会員データベース310に対して課金認証管理手段301より受け取った「会員ID」に対応する「会員使用可能金額」項目、並びに「決済記録」項目に対して「課金決済処理後の会員使用可能金額の書換え」「決済記録の追加書き込み」を要する。ここで、「課金決済処理後の会員使用可能金額」とは、例えば、会員使用可能金額から課金額を差し引いた金額、あるいは、会員使用可能金額から課金額、並びに、手数料等を差し引いた金額等を示す。

【0287】<手順36>会員データベース310は、要求のあった「会員ID」をキーワードに、データベース内の会員ユーザ情報の検索を実行し、同一の「会員ID」を発見した場合には、この「会員ID」に対応する「会員使用可能金額」項目、並びに「課金記録」項目に対して「課金処理後の会員使用可能金額の書換え」「課金記録の追加書き込み」を実行し、書換え、書き込み処理終了を課金処理手段304へ通知する。

【0288】なお、課金対象者12の課金決済については、課金対象者12が課金装置300を運用する課金サービス提供者と課金サービス提供契約を交わした際に指定した決済口座から、課金装置300が、会員データベース310に記録された課金記録に基づき、例えば、ある一定期間毎、あるいは、リアルタイムに引き落とすとしても良い。

【0289】また、課金サービス提供者が運営する課金装置300自体が決済機能を持っている場合ならば、会員データベース310を決済口座とし、会員IDに対応する会員使用可能金額を決済口座残高としても良い。こ

の場合、手順44、手順45で示す課金処理が課金対象者12への決済処理として機能する。

【0290】<手順37>課金手段304は、会員データベース310から書き込み終了通知を受け取ると、課金認証管理手段301へ課金処理正常終了として、課金処理報告する。また、課金手段303において課金処理不可と判定した場合には、課金認証管理手段301へ課金処理異常終了として課金処理報告する。

【0291】ここで、課金手段304から課金処理報告を受け取った課金認証管理手段301は、手順38～手順44、手順45～手順48の2つの手順を並行して実行する。

【0292】<手順38>～<手順44>課金決済処理後のサービス設備200の動作手順は、実施の形態6の手順48～手順54と同様である。

【0293】<手順45>～<手順48>課金決済処理後の移動体通信経由認証手段305の動作手順は、実施の形態6の手順55～手順58と同様である。

【0294】なお、本実施の形態では、図28の課金装置300の構成を特徴とする個人認証システムを応用したジュース自販機、切符券売機などの自販売機の課金システム、並びにそのサービスについて説明したが、本実施の形態で示した課金装置300を実施の形態7で示す定額有料施設の課金サービス、並びに、実施の形態8で示す時間制有料施設、駐車場に組み合わせることにより、サービス設備200と課金装置300間で事前に登録をすることなく、サービス設備200へのキャッシュレスサービスを実施する課金システムを構築できる。

【0295】

【発明の効果】上記実施の形態に示した個人認証システムにより、オープンな情報通信路で不正利用等により正規会員ユーザの会員ID番号および基本認証パスワード情報の不正取得が行われたとしても、会員ID番号に対応する移動体通信端末を同時に所有しない限り不正利用者による「成り済まし」の可能性を排除し、且つ、移動体通信端末を携帯する正規会員に対して不正なアクセスがあることを通知することができる。

【0296】また、実施の形態に示した個人認証システムを応用した課金システム、並びにそのサービスを用いることにより、例えば、父親が携帯する移動体端末の移動体端末呼び出し番号を移動体通信経由認証経由での認証対象として登録し、すべての会員IDとそれに対応する基本認証パスワード、移動体通信経由認証パスワードは、父親のみが知っており、子供には、一つの「会員ID」及び対応する「基本認証パスワード情報のみ」を覚えておくことにより、子供はサービス設備のサービスを、カードレス、キャッシュレスで享受することが可能である。また、この時、父親は、どこにいても、どここの「サービス設備」で、だれが、幾らのサービスを受



給費額を出しているかをリアルタイムで確認でき、かつ、その課金の可否を決定することが可能となる。

【図面の簡単な説明】

【図1】本発明の第1実施形態の個人認証システムを示す概念図

【図2】本発明の第1実施形態、第2実施形態、第3実施形態、第4実施形態および第5実施形態の個人認証システムにおけるサービス提供装置の構成を示す概念図

【図3】本発明の第1実施形態の個人認証システムを実現するために必要な会員ユーザ情報の例を示す図

【図4】本発明の第1実施形態の個人認証システムの認証手順を示したコラボレーション図

【図5】本発明の第2実施形態、第3実施形態、第4実施形態および第5実施形態の個人認証システムを示す概念図

【図6】本発明の第2実施形態、第3実施形態、第4実施形態および第5実施形態の個人認証システムを実現するために必要な会員ユーザ情報の例を示す図

【図7】本発明の第2実施形態の個人認証システムの認証手順を示したコラボレーション図

【図8】本発明の第3実施形態の個人認証システムの認証手順を示したコラボレーション図

【図9】本発明の第4実施形態の個人認証システムの認証手順を示したコラボレーション図

【図10】本発明の第5実施形態の個人認証システムの認証手順を示したコラボレーション図

【図11】本発明の第6実施形態、第7実施形態、第8実施形態、第9実施形態の個人認証システムを応用した課金システムの構成概念図

【図12】本発明の第6実施形態、第7実施形態、第8実施形態の個人認証システムを応用した課金システムの課金装置の構成を示す概念図

【図13】本発明の第6実施形態、第7実施形態、第8実施形態の個人認証システムを応用した課金システムを実現するために必要な会員ユーザ情報の例を示す図

【図14】本発明の第6実施形態、第7実施形態、第8実施形態の個人認証システムを応用した課金システムを実現するために必要な施設情報の例を示す図

【図15】本発明の第6実施形態の個人認証システムを応用した課金システムのサービス設備の構成を示す概念図

【図16】本発明の第6実施形態の個人認証システムを応用した課金システムを実現するために必要な物品情報の例を示す図

【図17】本発明の第6実施形態の個人認証システムを応用した課金システムの物理配置例を示す図

【図18】本発明の第6実施形態の個人認証システムを応用した課金システムの認証、課金手順を示したコラ

ボレーション図

【図19】本発明の第7実施形態の個人認証システムを応用した課金システムのサービス設備の構成を示す概念図

【図20】本発明の第7実施形態の個人認証システムを応用した課金システムを実現するために必要な物品情報の例を示す図

【図21】本発明の第7実施形態の個人認証システムを応用した課金システムの物理配置例を示す図

【図22】本発明の第7実施形態の個人認証システムを応用した課金システムの認証、課金手順を示したコラボレーション図

【図23】本発明の第8実施形態の個人認証システムを応用した課金システムのサービス設備の構成を示す概念図

【図24】本発明の第8実施形態の個人認証システムを応用した課金システムを実現するために必要な物品情報の例を示す図

【図25】本発明の第8実施形態の個人認証システムを応用した課金システムの物理配置例を示す図

【図26】本発明の第8実施形態の個人認証システムを応用した課金システムの入場時の認証手順を示したコラボレーション図

【図27】本発明の第8実施形態の個人認証システムを応用した課金システムの出場時の課金、認証手順を示したコラボレーション図

【図28】本発明の第9実施形態の個人認証システムを応用した課金システムの課金装置の構成を示す概念図

【図29】本発明の第9実施形態の個人認証システムを応用した課金システムを実現するために必要な会員ユーザ情報の例を示す図

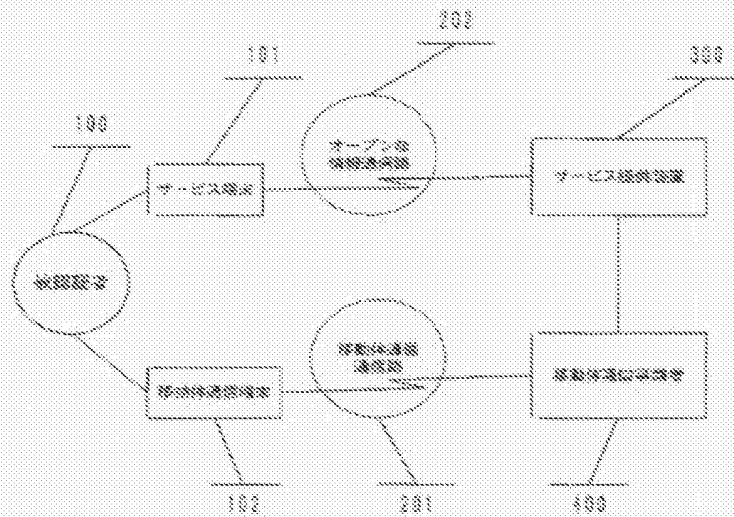
【図30】本発明の第9実施形態の個人認証システムを応用した課金システムの出場時の課金、認証手順を示したコラボレーション図

【符号の説明】

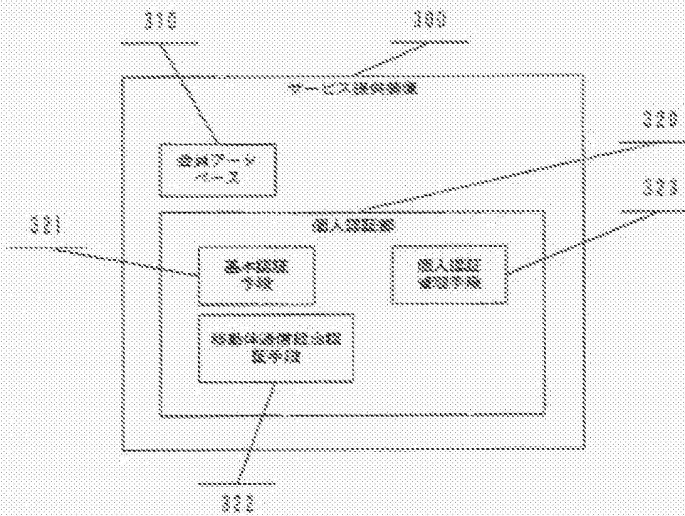
- 100 被認証者
- 101 サービス端末
- 102 移動体通信端末
- 201 移動体通信通信路
- 202 オープンな情報通信路
- 203 サービス端末、移動体通信端末間通信路
- 300 サービス提供装置
- 310 会員データベース
- 320 個人認証部
- 321 基本設定手段
- 322 移動体通信経由認証手段
- 323 個人認証管理手段
- 400 移動体通信事業者



【図1】



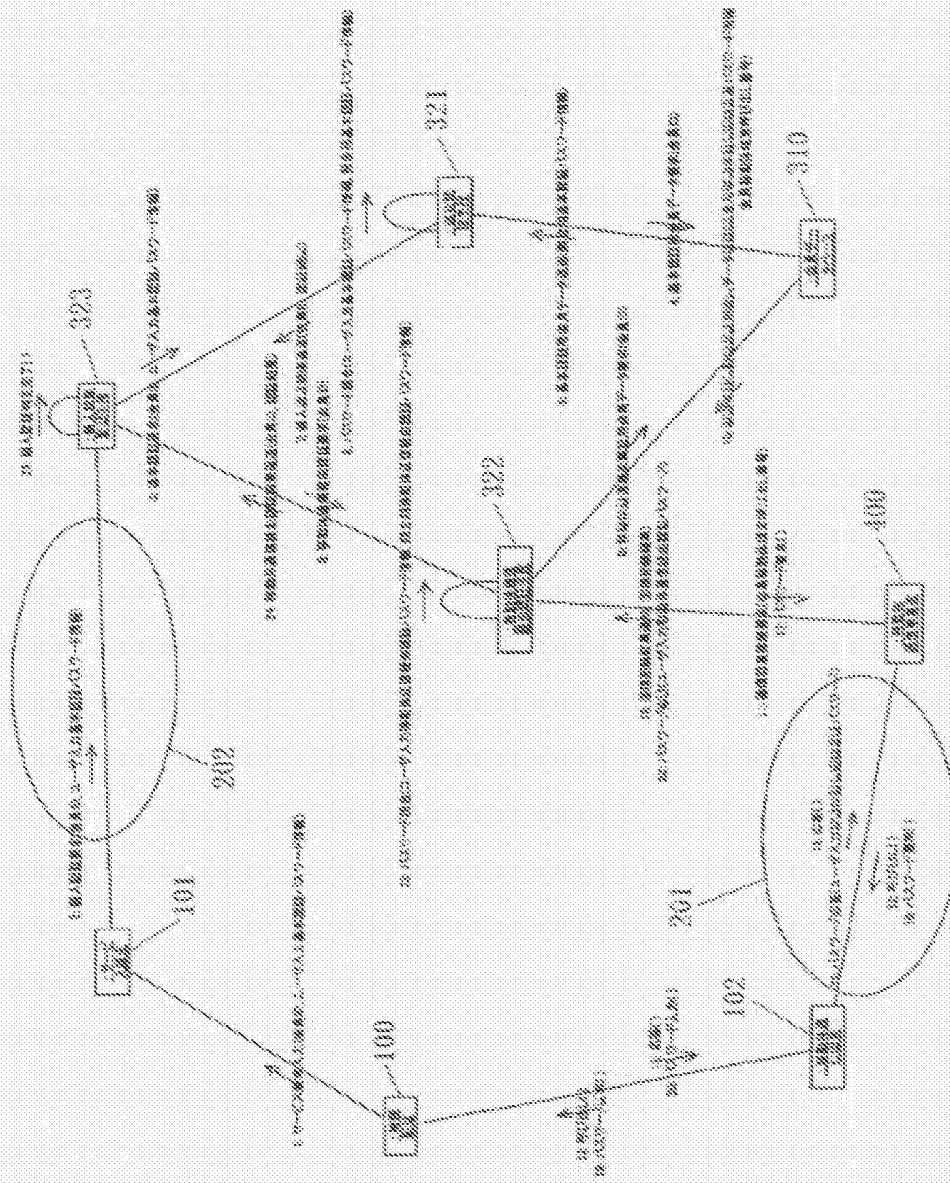
【図2】



【図3】

会員氏名	会員ID番号	基本認証 パスワード情報	移動体通信端末 呼び出し番号	移動体通信端末認証 パスワード情報
横田	YABE	GT104	060211	0023
小林	KIRO	GT110	095320	0060
横田	KICHI	GT112	0952300	4046

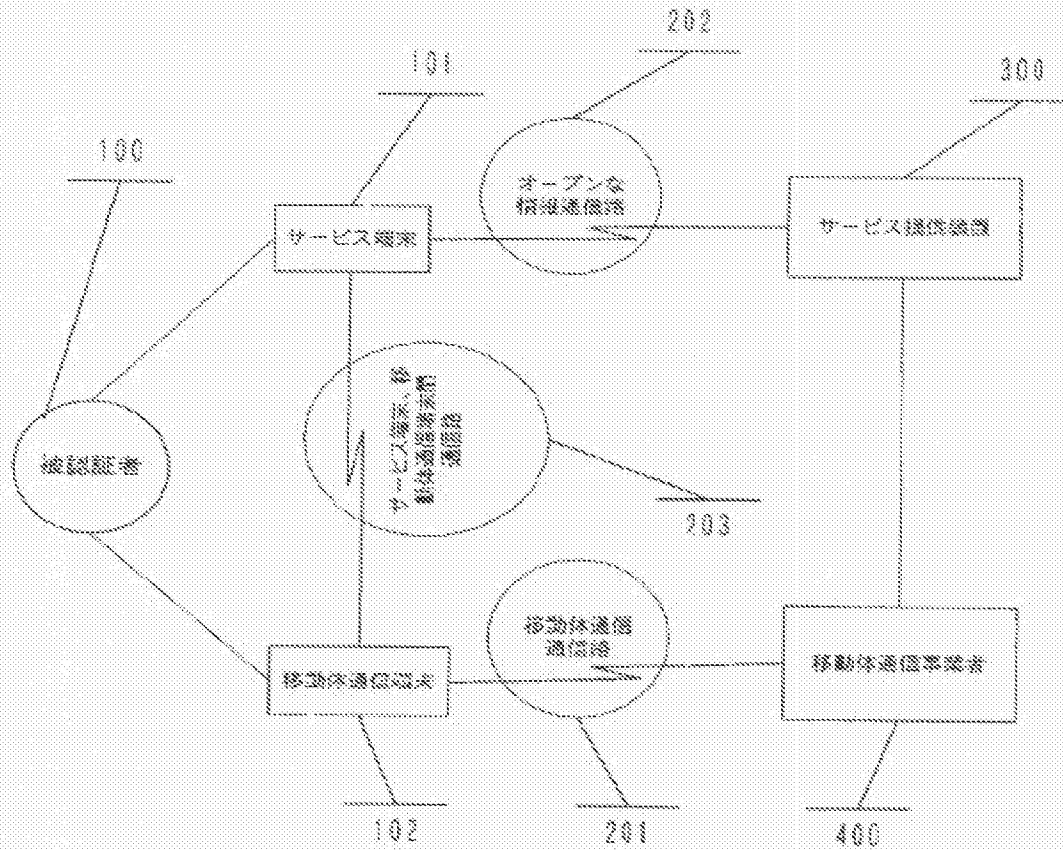
1044



10134

[illegible]

【図5】



【図6】

会員ID番号	基本料金用 パスワード情報	移動体通信料金証明用 パスワード情報
NADE	QT104	3023
HIRO	QT110	8068
KICHI	QT112	4068

【図16】

設備管理DB例（自販機、または、事前チケット購入等の場合）

選択可能サービス名称	料金額
アイソップ	120円 / 本
ペプシ	120円 / 本
缶装（ペットボトル）	140円 / 本



【図8】

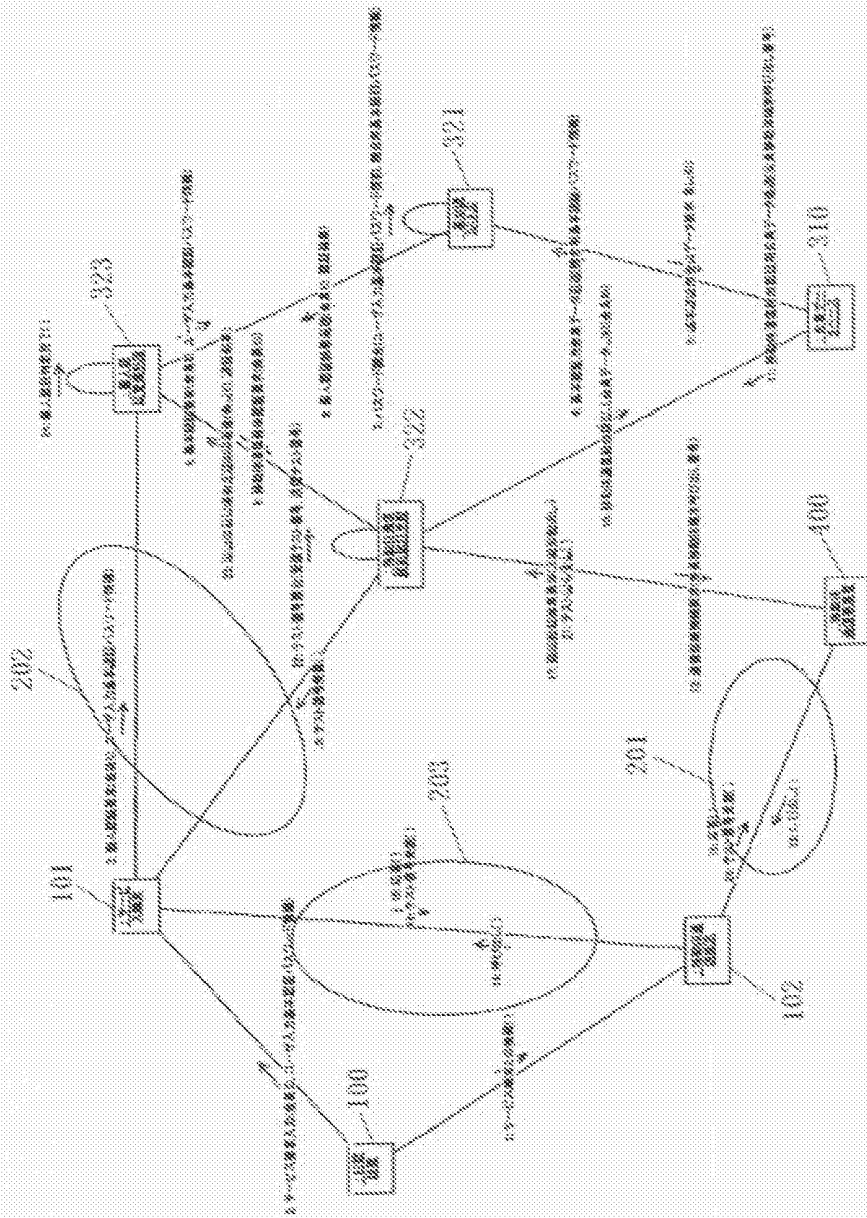
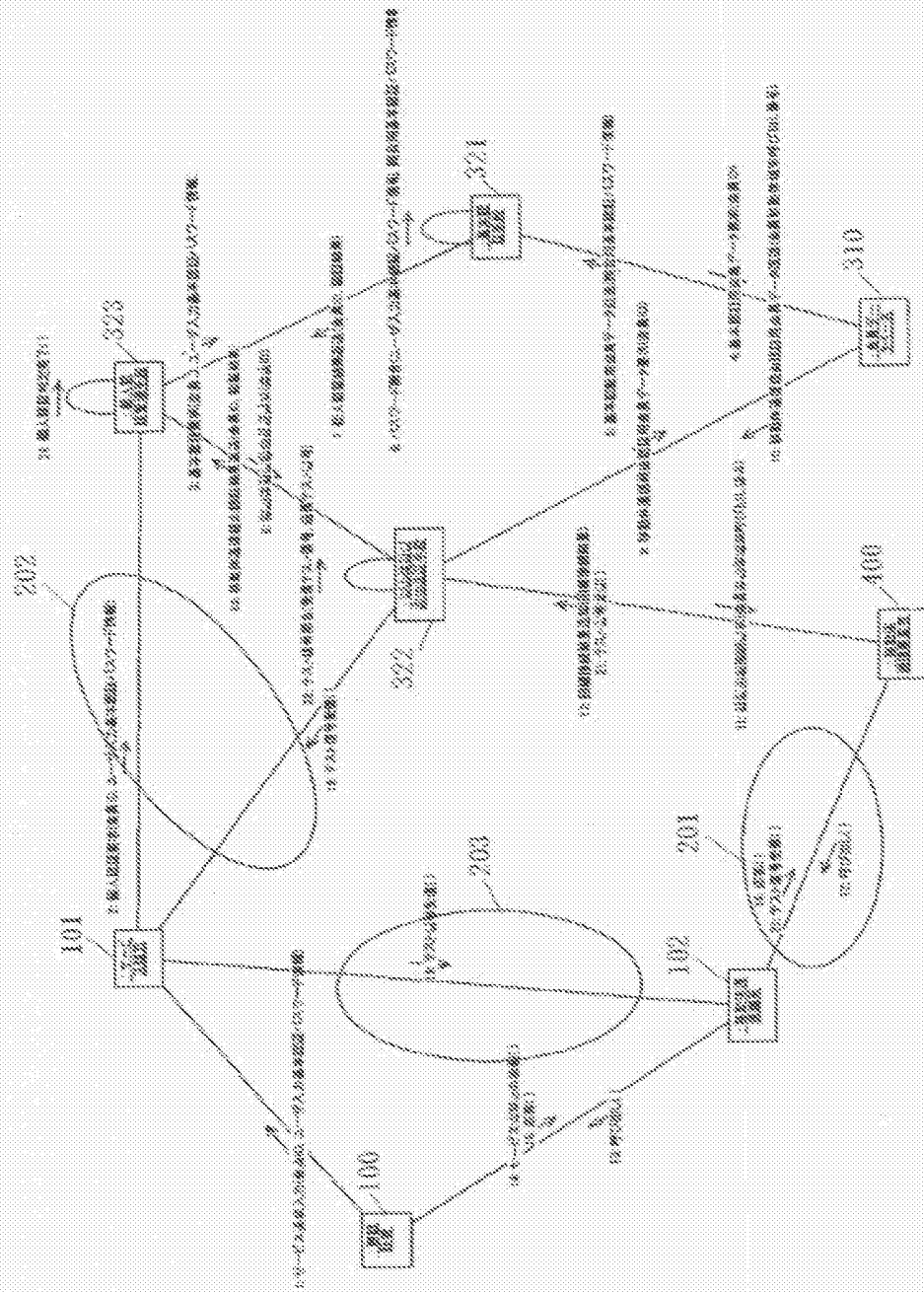


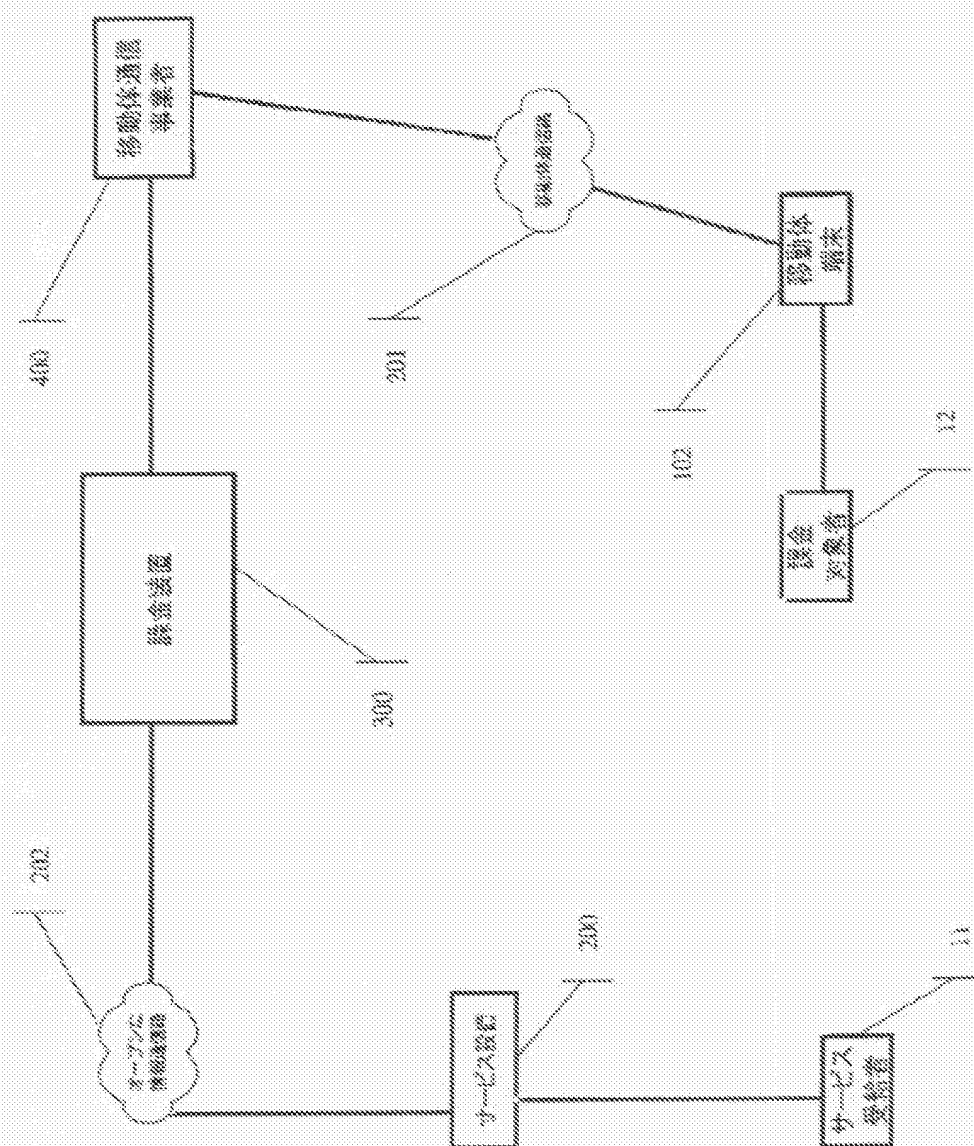




図10

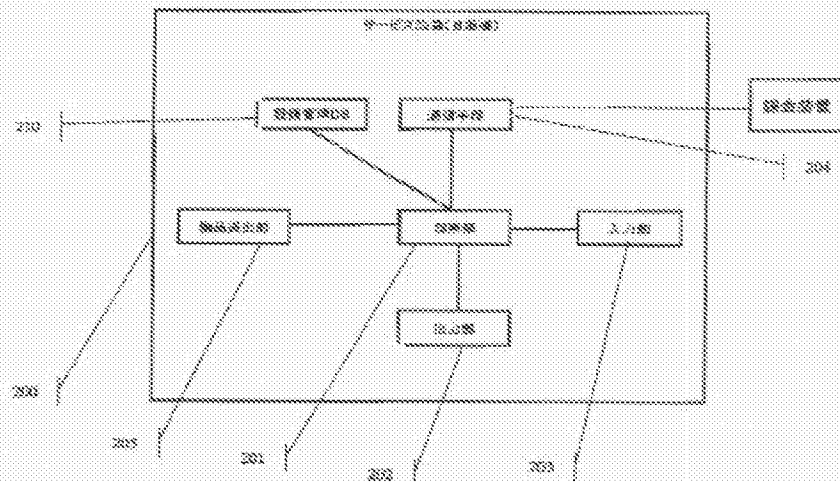


【図11】

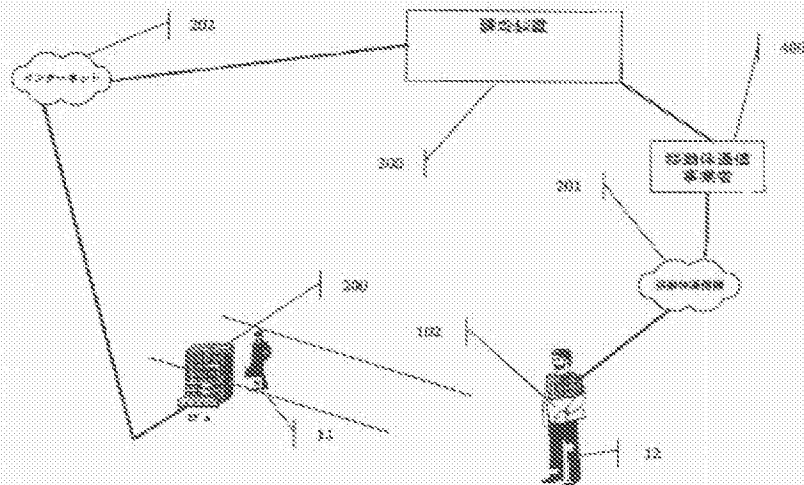




【図15】



【図17】

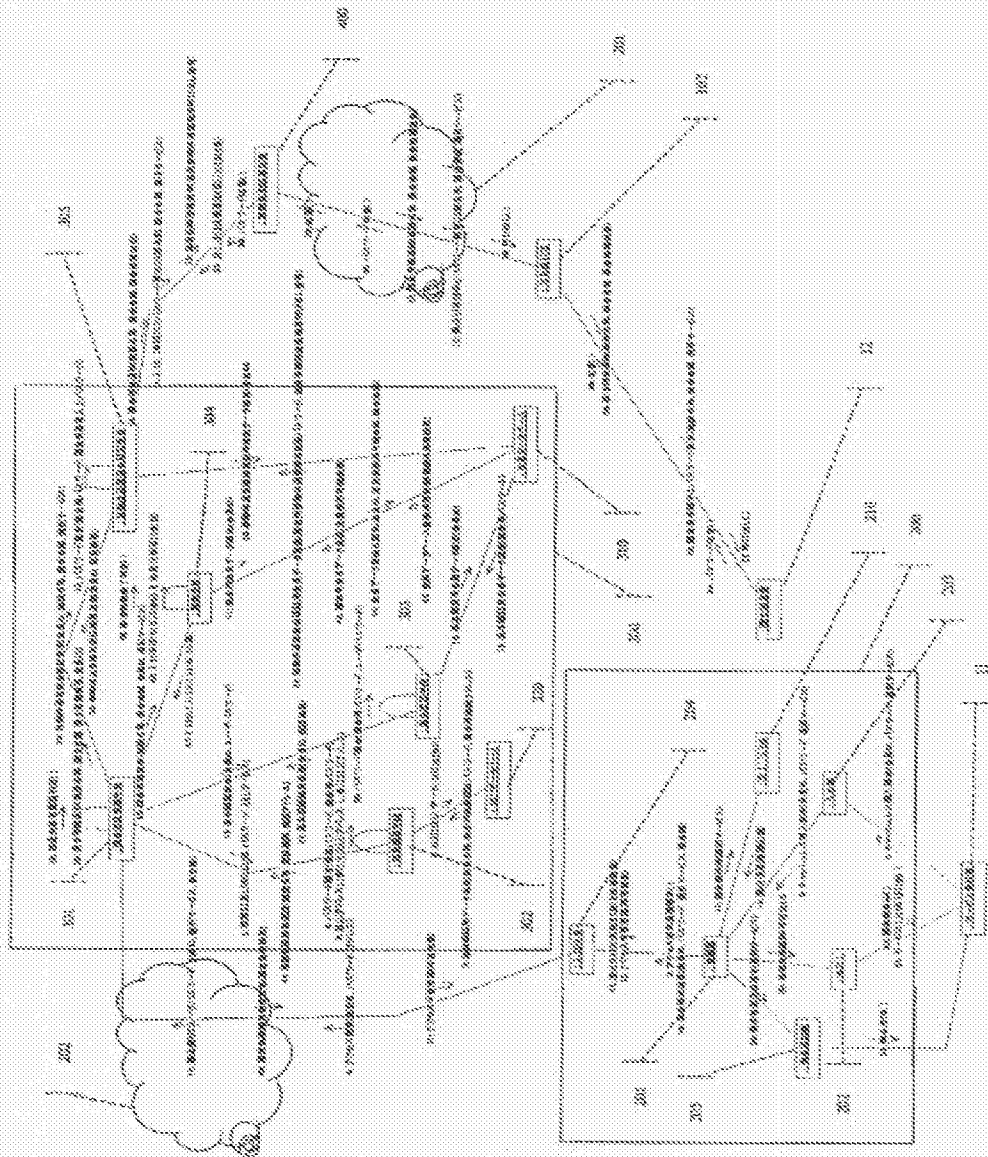


【図20】

設備管理DB例 (定額有料施設)

施設可能サービス名称	課金額
おとな (オールデイ)	5400 円
おとな (トワイライト)	3800 円
こども (オールデイ)	2000 円
こども (オールデイ)	1800 円

FIG. 10

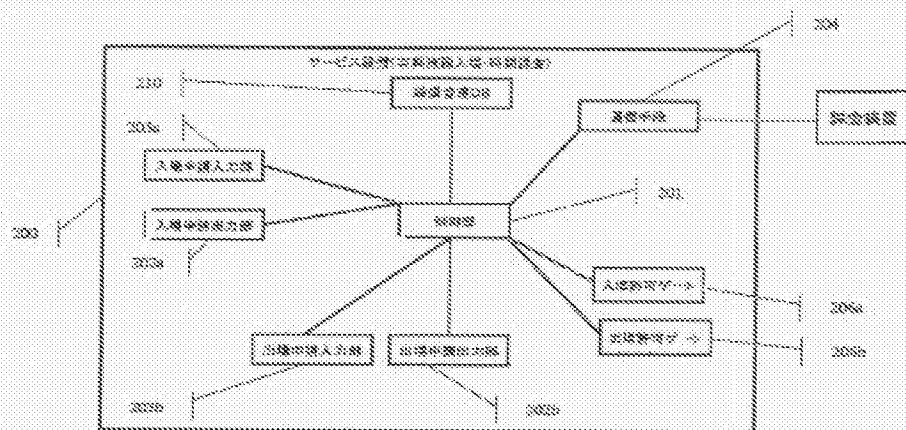




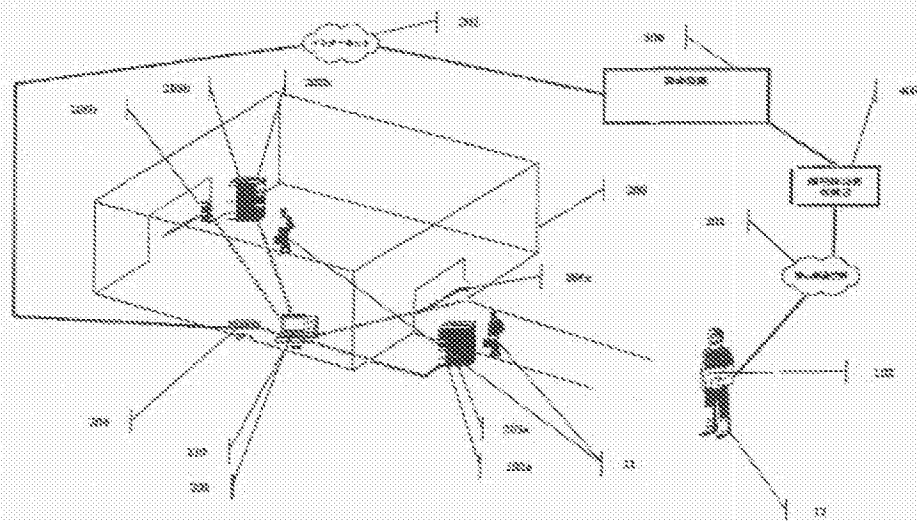




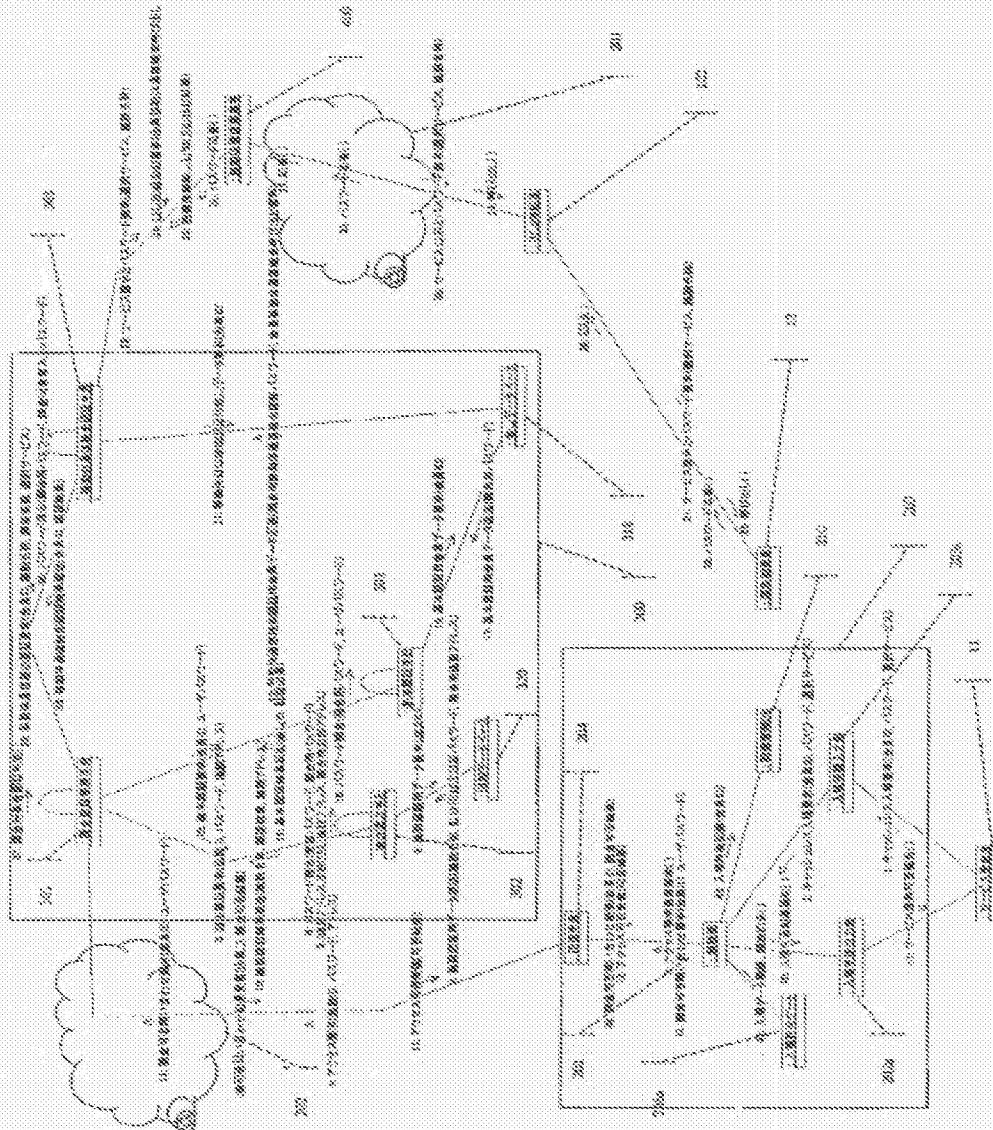
1000000

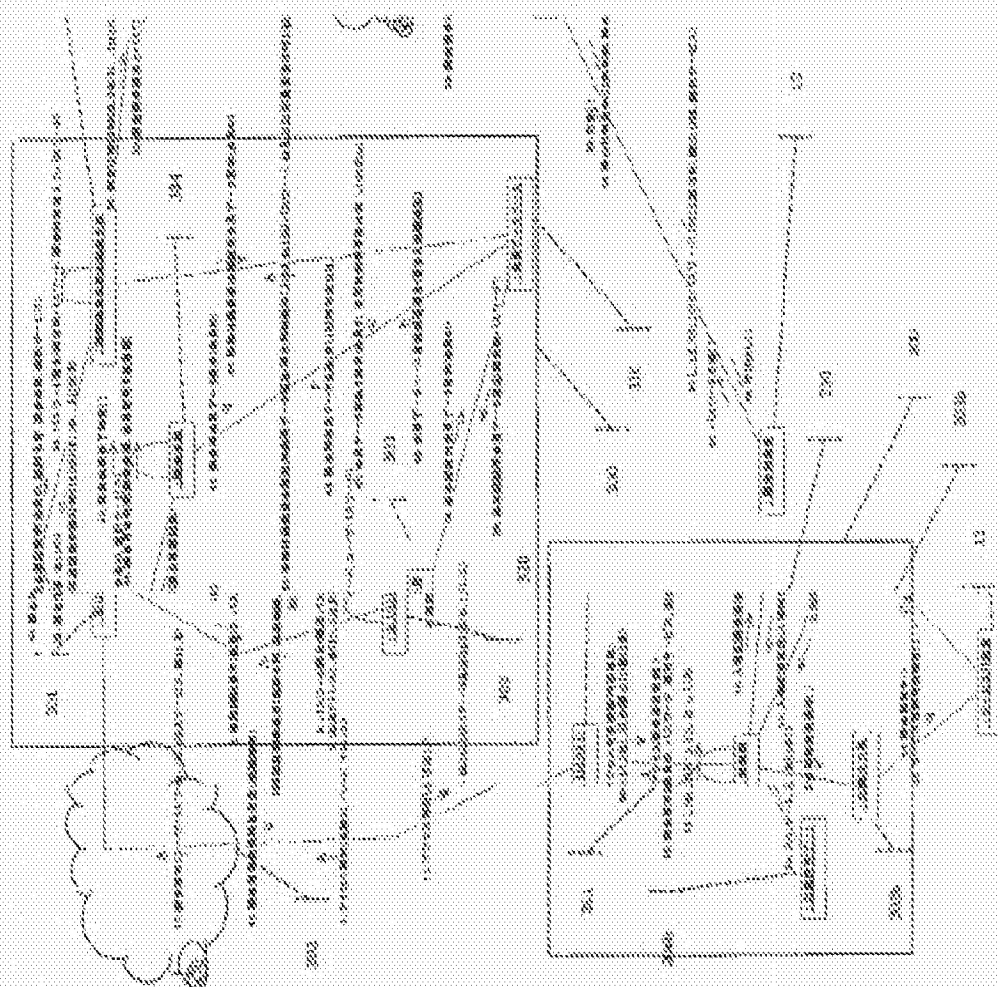


110051

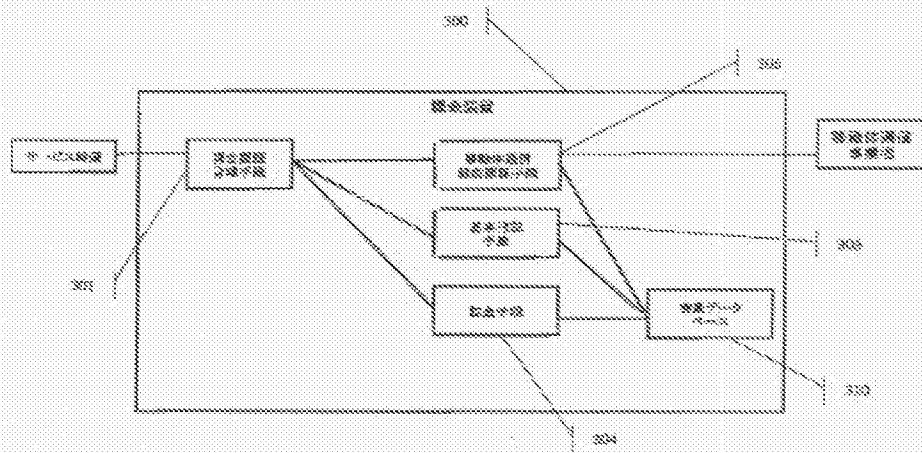


(36) 01





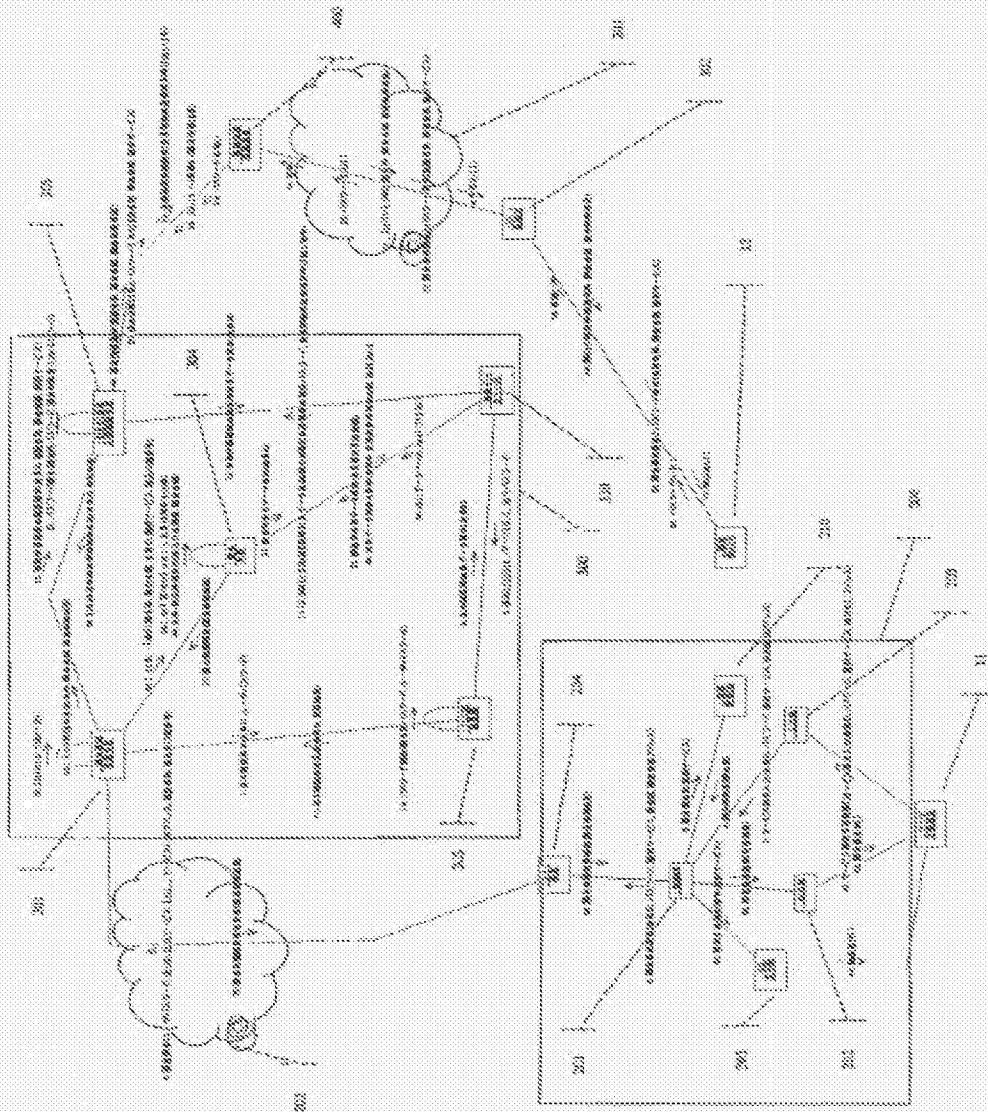
【図28】



[illegible]



【図30】



フロントページの続き

(50)Int.Cl.

H04Q 7/38

発明の要約

FI

H04B 7/26

H04Q 7/04

1093

H

(参考)